Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives
Arnbak, A.M.

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: http://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.
Securing Private Communications


ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. D.C. van den Boom
ten overstaan van een door het college voor promoties
ingestelde commissie, in het openbaar te verdedigen in de Aula der Universiteit
op woensdag 25 november 2015, te 11:00 uur
door

Axel Martin Arnbak

geboren te ’s-Gravenhage
Promotiecommissie:
Promotor: Prof. dr. N.A.N.M. van Eijk, Universiteit van Amsterdam.
Copromotor: Prof. dr. N.E. Helberger, Universiteit van Amsterdam.
Overige leden: Prof. mr. E.J. Dommering, Universiteit van Amsterdam.
Prof. dr. P.A.L. Ducheine, Universiteit van Amsterdam.
Prof. dr. M.J.G. van Eeten, Technische Universiteit Delft.
Prof. dr. U. Gasser, Harvard University.
Prof. dr. B.P.F. Jacobs, Radboud Universiteit Nijmegen.

Faculteit der Rechtsgeleerdheid
### Concise Table of Contents

1. Introduction ........................................................................................................... 8

PART I: A HISTORY OF EU COMMUNICATIONS SECURITY LAW .... 28

2. Five EU Communications Security ‘Policy Cycles’ .............................................. 28

3. Analytical Framework ......................................................................................... 80

PART II: THEORY AND TOOLS FOR THE EU LAWMAKER .................. 100

4. Fundamental Rights Perspectives ........................................................................ 100

5. Systems Design Perspectives ............................................................................. 154

6. Political Perspectives .......................................................................................... 180

PART III: CASE STUDIES FOR THE EU LAWMAKER ......................... 198

7. Model and Methodology ....................................................................................... 198

8. HTTPS – Communications Security in Web Browsing ..................................... 202

9. The Snowden Files – Communications Security in the ‘Cloud’ ................. 244

PART IV: SECURING PRIVATE COMMUNICATIONS ............................ 303

10. Summary, Analysis and Conclusions ................................................................. 303

References ................................................................................................................. 351

Short summary in Dutch ............................................................................................ 371

Acknowledgements .................................................................................................... 378
Table of Contents

1. Introduction ........................................................................................................ 8
   1.1. Research Question ....................................................................................... 16
   1.2. Methodology and Limitations .................................................................... 19
   1.3. Scope .......................................................................................................... 23
   1.4. Outline ....................................................................................................... 25

PART I: A HISTORY OF EU COMMUNICATIONS SECURITY LAW .... 28

2. Five EU Communications Security ‘Policy Cycles’ ........................................... 28
   2.1. Information Systems & Critical Infrastructures ....................................... 31
   2.2. Data Protection ......................................................................................... 38
   2.3. The Telecoms Package ............................................................................. 42
   2.4. Digital Signatures and Certificates ........................................................... 51
   2.5. Cybercrime ................................................................................................ 57
   2.6. The Proposed ‘Network and Information Security’ Directive ............... 63
   2.7. Historical Analysis of EU Communications Security Law ................. 71
   2.8. Conclusion ................................................................................................ 76

3. Analytical Framework ....................................................................................... 80
   3.1. Definitions: Conceptual Ambiguity ............................................................ 80
   3.2. Scope: ‘Personal Data’ and ‘Actors’ ......................................................... 86
   3.3. Security Strategies: Deterrence vis-à-vis Protection .................................. 93
   3.4. The EU, Communications Security and National Security ................. 94
   3.5. Summary ................................................................................................... 97

PART II: THEORY AND TOOLS FOR THE EU LAWMAKER ........... 100
4. Fundamental Rights Perspectives ............................................................. 100
4.1. European Fundamental Rights Law and Positive Rights .................. 102
4.2. Positive Obligations to Protect Communications Security ............. 109
4.3. A Living Instrument: Scoping ‘Communications’ Functionally ....... 124
4.5. Protection Against Arbitrary National Security Interferences ......... 141
4.6. Legislatures’ System Responsibility to Protect ................................. 148
4.7. Conclusion .......................................................................................... 151

5. Systems Design Perspectives ................................................................... 154
5.1. The Technical Conception of ‘Security’: The c.i.a.-Triad ............... 155
5.2. The Centrality of ‘Authorization’ .......................................................... 162
5.3. Security Requirements Engineering .................................................... 165
5.4. Failure Classes: Surveillance, Users, Technology, Markets .......... 171
5.5. Security Economics ............................................................................ 175
5.6. Conclusion .......................................................................................... 177

6. Political Perspectives .............................................................................. 180
6.1. The Political Conception of ‘Security’ ................................................ 181
6.3. ‘Cyber’ Securitization ....................................................................... 189
6.4. Implicit Politics of Technical Policymaking ...................................... 192
6.5. Conclusion .......................................................................................... 195

PART III: CASE STUDIES FOR THE EU LAWMAKER ......................... 198

7. Model and Methodology ......................................................................... 198

8. HTTPS – Communications Security in Web Browsing ....................... 202
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1. The HTTPS Communications Value Chain</td>
<td>204</td>
</tr>
<tr>
<td>8.2. Incidents and Systemic Vulnerabilities</td>
<td>211</td>
</tr>
<tr>
<td>8.3. Incentives</td>
<td>218</td>
</tr>
<tr>
<td>8.4. The c.i.a.-Triad in HTTPS</td>
<td>225</td>
</tr>
<tr>
<td>8.5. Technical Solutions</td>
<td>228</td>
</tr>
<tr>
<td>8.6. Current and Proposed EU Legislation</td>
<td>231</td>
</tr>
<tr>
<td>8.7. Conclusion</td>
<td>240</td>
</tr>
<tr>
<td>9. The Snowden Files – Communications Security in the ‘Cloud’</td>
<td>244</td>
</tr>
<tr>
<td>9.1. Intra- and Interdomain ‘Cloud’ Communications Value Chains</td>
<td>247</td>
</tr>
<tr>
<td>9.2. Incidents and Systemic Vulnerabilities</td>
<td>256</td>
</tr>
<tr>
<td>9.3. Incentives</td>
<td>270</td>
</tr>
<tr>
<td>9.4. The c.i.a.-Triad in Cloud Communications</td>
<td>279</td>
</tr>
<tr>
<td>9.5. Technical Solutions</td>
<td>293</td>
</tr>
<tr>
<td>9.6. Current and Proposed EU Legislation</td>
<td>294</td>
</tr>
<tr>
<td>9.7. Conclusion</td>
<td>299</td>
</tr>
<tr>
<td>PART IV: SECURING PRIVATE COMMUNICATIONS</td>
<td>303</td>
</tr>
<tr>
<td>10. Summary, Analysis and Conclusions</td>
<td>303</td>
</tr>
<tr>
<td>10.2. Part II: Theory and Tools for the EU Lawmaker</td>
<td>312</td>
</tr>
<tr>
<td>10.3. Part III: Case Studies for the EU Lawmaker</td>
<td>330</td>
</tr>
<tr>
<td>10.4. Conclusion, Recommendations and Outlook</td>
<td>336</td>
</tr>
<tr>
<td>References</td>
<td>351</td>
</tr>
<tr>
<td>Short summary in Dutch</td>
<td>371</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>378</td>
</tr>
</tbody>
</table>
1. Introduction

On a warm summer night in 2011, the Dutch Minister for Internal Affairs was called in by his staff to deliver an ad hoc press conference on a Saturday, well after midnight.\(^1\) When the announcement was made, social media exploded: had the coalition fallen apart? Were the Belgians invading Maastricht? Had the dikes collapsed and were the Lower Countries in for watercalyptic mayhem? Well, to some extent the latter had occurred: Minister Donner announced to the world that the Internet was broken and could no longer be trusted. But, he added, the Dutch Government was ready to save the day. In the meantime, people should “write letters and bank checks, just like me.”\(^2\)

The DigiNotar-affair paralyzed secure networked communications in the Netherlands for a week, made the Government seize a privately-owned company on a dubious legal basis, purportedly breached the Gmail communications of 300,000 Iranian Internet users, and according to an official EU report may have caused Iranian activists to be imprisoned or even killed.\(^3\) As nobody could tell to what extent Dutch hospitals, the Rotterdam harbor – one of the world’s largest – and other critical infrastructure depended on DigiNotar’s services, the Government convinced Microsoft to delay essential software updates for one week in the Dutch market. Years later, based on a top-secret slide deck leaked by former US intelligence analyst Edward Snowden, security experts and Dutch media would speculate whether British and US intelligence agencies either helped to attribute the cyberattack to the Iranian government, or even piggybacked on the vulnerability in order to eavesdrop on

\(^1\) For an extensive account of the DigiNotar affair, see section 8.2 and Arnbak & Van Eijk 2012.
\(^3\) ENISA 2011.
the communications of millions of Internet users, companies and public institutions.⁴

The disclosures by Mr. Edward Snowden have indeed driven the point home that any communicative act online is at risk to be breached by a myriad of intelligence agencies, along with a sprawling swarm of cybercriminals, advertising networks, employers, corporate data-miners, and then some. Spectacular interconnectivity, increasing dependence and claims of a “fourth revolutions” in human organization where “existence is information” notwithstanding, ⁵ networked communications seem systemically insecure. Even the specific vulnerabilities and damages emerging from the DigiNotar-affair in 2011 and the Snowden-saga since 2013 – extensively researched in Part III of this study – are far from being addressed.

Decades into weaving the World Wide Web, a sobering picture emerges about the state of fundamental rights in the networked environment. The lack of privacy and communications security is lamented across cultures, around the globe.⁶ But large percentages of concerned users see no other choice than to hop onto the web-based bandwagon, ⁷ infamously transforming from a consumer to a product – or a surveillance target – in the process. They have come to depend on a networked communications environment that is fundamentally insecure. In addition to fundamental rights, cybercrime has become a major concern. While estimates are notoriously untrustworthy, damages run into the billions of Euros per annum.⁸ Conventionally, and cybercrime is no exception, law responds to surges in crime by creating new investigative powers and tougher sanctions, while minor offenders are caught

⁵ Floridi 2014.
⁶ CIGI 2014.
⁷ Pew 2014.
⁸ Anderson et. al. 2012.
with much fanfare to “set an example”. But such strategies of deterrence have proven to be ineffective and were always recognized as such, even in the preambles of the first international Cybercrime Convention.\textsuperscript{9} Meanwhile, the inertia displayed by communications providers and legislatures to implement basic communications security measures and ensure fundamental rights has created a fertile investment environment to acquire evermore advanced cybercrime techniques and capacity.\textsuperscript{10} To make matters even more complicated, leaked documents show that the NSA – the US intelligence agency responsible for both signals intelligence and communications security – piggybacks on cybercriminals that piggyback on insecure communications. Operation DEFIANTWARRIOR is but one example, in which the NSA uses technologies codenamed QUANTUMBOT to covertly co-opt botnets created by cybercriminals and other intelligence agencies for the purposes of signals intelligence.\textsuperscript{11} Leaky apps, such as the wildly popular game Angrybirds that was downloaded over 1.7 billion times across platforms in January 2014, serve as a “golden nugget” for communications surveillance by the NSA.\textsuperscript{12} Far from being exclusively a technical issue, securing private communications is about law, policy, economic incentives, and even war and peace too.

Security itself is a ‘slippery’ concept.\textsuperscript{13} Unsurprisingly, stakeholders across the policy spectrum – politicians, corporations, security experts, judges and so on – appeal to different conceptions of ‘communications security’ when they speak security. Technical security is primarily the domain of computer experts, who have studied the issue since the 1960s, seeking to protect the confidentiality, integrity and availability of systems and communications. The newer concept of ‘cybersecurity’ was launched by the US intelligence community in the US

\textsuperscript{9} See section 2.5
\textsuperscript{10} Bruntom 2015.
\textsuperscript{11} See <http://www.spiegel.de/media/media-35689.pdf>, accessed 1 September 2015.
\textsuperscript{13} Zedner 2003. See extensively section 5.1.
political arena in the mid-1990s, and according to Nissenbaum is used as a dominant term to frame policy efforts to serve national security and economic interests. Indeed, the intelligence establishments around the world increasingly argue that “in order to defend the nation against cyberattacks, we need to monitor all communications”. Even if NATO has started to develop manuals for creating international standards that should regulate military conduct in global cyberspace, today cyber warfare is not so much ruled by law, but by game theory: the probabilities of getting caught. As such, we witness defense and attack of communications infrastructure, all in the name of ‘security’. This study analyzes how the political (chapter 6), technical (chapter 5) and core fundamental rights conceptions of security (chapter 4) interact and could be balanced in Part II.

Amidst security incidents and surveillance sagas, market operators are responding to growing user concern post-Snowden by proposing and even implementing basic security measures. Early-adopting Internet companies are starting to implement basic encryption technologies, for instance when communicating with users (HTTPS), between datacenters, and between providers (STARTTLS for e-mail). Device manufacturers implement smartphone encryption in ways that only users get the key. Meanwhile, intelligence and law enforcement agencies, as well as UK Prime Minister David Cameron and US President Barack Obama now call for mandated backdoors into all electronic communications. Their policy response spurred a

16 NATO 2009.
17 Axelrod & Illiev 2014.
18 See chapter 4 and 5.
19 See chapter 9.
20 Arnbak & Goldberg 2015.
21 See chapter 9.
sharp reaction from fourteen leading computer scientists, calling “proposals for
exceptional access wrong in principle and unworkable in practice”. The
competing interests in communications security will once again, twenty years
after the first crypto wars of the 1990s, lead to an intense political battle on
communications security. Whereas the 1990s crypto wars were fought over the
technological means to encrypt in and of itself, today the general
implementation of robust communications security technologies is at stake in
what has been dubbed the “crypto wars 2.0”, extensively discussed in chapter 9.
More generally, the last quarter century of EU communications security
policymaking, particularly around the 1990s, holds insightful lessons for
communications security policymaking today – analyzed in chapter 2.

Added protective measures such as encryption have become commonplace
today, because the technical foundations of networked communications have
never prioritized security. The communications protocols that enable machines
to form the network of networks we call ‘the Internet’ and speak to each other
– such as HTTP and BGP\textsuperscript{24} – have from the outset not been designed with
security as a priority, but connectivity. Moreover, nearly every single piece of
software must at some point trust input from other software. Upon receiving
the 1984 ACM Alan Turing Award, Ken Thompson famously showed that

\begin{flushright}
\textsuperscript{23} Abelson et. al. 2015. Quote taken from <http://www.nytimes.com/2015/07/08/technology/code-specialists- oppose-us-and-british-
government-access-to-encrypted-communication.html?_r=0>, accessed 1 September 2015. See also Arnbak 2014a.
\textsuperscript{24} The HyperText Transfer Protocol underlies server-to-server communication and has enabled
the World Wide Web as we know it today. See: <http://www.w3.org/Protocols/HTTP/AsImplemented.html>, accessed 1 September 2015. Its
security update HTTPS is extensively studied in chapter 8. The Border Gateway Protocol enables
communication between networks – called Autonomous Systems – owned by different
organizations. See Rekhter & Li 1995. BGP is extensively discussed the ‘cloud communications’
chapter of chapter 9.
\end{flushright}
“trusting trust” implies inherent exposure to vulnerability. In addition to trusting trust, convergence, rise of interconnectivity, and a spectacular increase in software complexity exacerbate the inherent presence of technical vulnerabilities in ICTs. Completely understanding, predicting and controlling vulnerabilities in the networked communications environment is beyond anyone.

Many technical fixes already exist for well-known vulnerabilities in core Internet protocols, software and hardware. And in the aftermath of a breach, the general public usually learns that it was not the lack of available technical fixes, but a lack of incentive on part of the breached entity that caused communications security to fail. For example, shortly after the POODLE bug was published, which allowed an attacker to steal unencrypted communications from purportedly encrypted communications through HTTPS, it became clear Citibank has been affected. Until late 2014, at least, its webservers relied on SSLv3, a cryptographic protocol that had become outdated fifteen years ago by the introduction of its successor TLS v.1.0. Why update ICT that just ‘works’ to enhance communications security for your customers, even if just because you are one of the largest financial institutions in the world? Why take on surplus investments for security and fallback scenarios? What could possibly go wrong?


26 See <https://poodle.io/>
27 See <https://poodle.io/>, For excellent commentary on how POODLE demonstrates the fundamental market failures of web browsing security, see Bonneau 2014.
Law is one of the tools in contemporary democratic society to mediate the complex interactions between national security, shareholder value, innovation and freedom. After a relatively hands-off approach around the globe in recent decades, lawmakers worldwide are gearing up to intervene. Legal scholarship on the subject is sparse, however. In the EU, even a clear overview of current EU communications security law is lacking. Nobody seems to know what EU laws regulate communications security, even specially commissioned researchers that are supposed to map the policy space.\textsuperscript{29} Even so, the EU has launched or adopted a range of legislative proposals over the last years that will have deep implications for communications security in the coming decade, far beyond Europe’s borders. In chapter 2, this study offers the first historical analysis in the academic literature of the last 25 years of EU communications security law.

The debate about the viability of EU law to secure communications is rapidly intensifying. Supporters of regulatory intervention can be found in the relatively new but influential field of security economics. Here, it is argued that communications security often fails because damage of breaches are not suffered on the supply-side of the market.\textsuperscript{30} Employing classic economic theories around market failure and empirical methodologies, security economics research aims to uncover where regulatory intervention is essential to organize the incentives in communications security markets in the public interest. Information asymmetries, lock-in, liability dumping and negative externalities can be addressed by regulatory schemes that mandate security requirements, breach notifications and liability distribution and thus optimize security in the public interest.

\textsuperscript{29} For example, N. Robinson et al. 2013.
\textsuperscript{30} See chapter 5, particularly section 5.5.
Moreover, private communications security is instrumental for the enjoyment of fundamental rights. In chapter 4, this study uncovers that the courts of the Council of Europe and European Union are developing positive human rights obligations for the EU lawmaker to secure communications through legislation and enforcement. As this ‘new’ fundamental right is in its infancy, open questions remain how to conceptualize ‘private communications security’ and how it should be implemented in current and future EU legislation. One pressing example is the definition of ‘communications’; the scope of the central instrument in EU communications law – the Telecoms Package – is limited to conventional telecommunications and Internet access providers, rather than relatively new but increasingly relevant ones, such as messaging apps, webmail and VoIP providers. In other words, if you send an e-mail through your Internet access provider’s e-mail account, the communications confidentiality and breach notification safeguards of the E-Privacy Directive apply, but if you use Gmail, they don’t. The approach seems untenable going forward. The conceptualization of private communications security – its definition, scope, provisions and enforcement – is one of the main research topics of this study.

On the other hand, legislative approaches to augment communications security have fierce opponents. Several legal proposals to ostensibly secure communications reinforce or expose networked communications to well-known security vulnerabilities, rather than resolving them, such as Internet driving licenses and Internet kill switches.31 Traditionally, technical experts voice more radical concerns, and believe that communications security is lost as soon as law touches it. However, the lofty image of ‘code rebels beating the

---

31 Opderbeck 2012. President Obama’s internet kill switch entails a full-stop button for internet communications when a DDoS-attack takes place. The proposal completely sidesteps the security implications of re-engineering the decentralized network of networks (the internet) into a centralized network where a single entity has the control to stop the internet. And the political implications of what would happen if that power is used erroneously, or falls in the hands of whoever hacks an internet kill switch.
government – saving privacy in the digital age” that emerged from the 1990s crypto wars seems desperately naïve, comfortably numbing Internet engineers into thinking the day was saved by perfect mathematical concepts. Now the world knows that theoretically sound cryptography has been deeply subverted in its implementation into security technologies and protocols. More than any other Snowden disclosure, operation BULLRUN spurred a furious reaction in technical communities. The BULLRUN program illuminates how law, technology and political organization interact in complex ways, but are all required to ensure enjoyment of basic freedoms and secure networked communications. And physical security too, when not only our communications but our ‘things’ – such as refrigerators, cars and pacemakers – are networked too. The successful compromise of FiatChrysler Jeep through its Internet-connected entertainment system uConnect, effectively giving security researchers the ability to accelerate, steer and stop a driving car from behind their laptops, provides perhaps the most compelling real life example of the profound consequences of communications security breaches to come.

1.1. Research Question

Against the background sketched in the introduction, this study is organized around the following central research question:

*How should the EU lawmaker protect private communications security?*

One of the main aims of this study is to provide clear definitions through conceptual analysis of terms such as ‘communication’ and ‘security’. A first outline of the terminology of the research question is offered in this section.

---

33 Arnbak 2015.
With the term ‘the EU lawmaker’, this study chooses the legal system of the European Union as its primary object of research, as well as the role of the EU institutions in this rapidly evolving policy area. As a clear overview of current law is lacking in scholarly and policy communities, a historical analysis is conducted into relevant EU law in chapter 2. The study identifies five so-called ‘policy cycles’ and outlines their definition of ‘security’, scope and provisions and enforcement structures. The cycles identified are: network and information security, data protection, the Telecoms Package, digital signatures and certificates, and cybercrime. National security, excluded from the EU’s regulatory competence, has not been identified as a separate policy cycle, but the study shows its major explicit, implicit and secret impact across these five policy cycles. The study argues that the EU lawmaker needs to develop a new stance towards national security if it is to meet fundamental rights obligations, as the European Convention of Human Rights (‘ECHR’) and in particular the EU Charter on Fundamental Rights adopted in 2009 form an integral part of EU law. The fundamental rights perspective of private communications security is analyzed in chapter 4 of the study.

‘Security’ is a highly ambiguous, overloaded and ‘slippery’ term.\textsuperscript{34} In EU law, security sometimes refers to the technical concept of assuring confidentiality, integrity and availability for authorized entities.\textsuperscript{35} More prominently, security features in its political guise that relates to war and peace, one of the primary functions of government since its inception. As one of the oldest legal concepts around, the technical and political conceptions of ‘security’ are researched in chapter 5 and 6 of this study.\textsuperscript{36}

\textsuperscript{34} Zedner 2003, p. 154.
\textsuperscript{35} Pfleeger 2003.
\textsuperscript{36} See section 3.3.
With the element ‘private communications’, the study researches electronic communications technologies of the networked environment. The study will mainly analyze private communications security from the perspective of citizens. Then again, many of the findings extend beyond the citizen to other entities. For instance, where the study reflects on the persistent market failures in communications security production for the demand-side of the market, these market failures affect the private communications of citizens, corporations and governments alike.

Two conceptions of ‘communications’ exist in European law. In the Telecoms package, a narrow ‘actor-based’ approach includes a narrow set of providers within the concept of ‘communications’, primarily those offered by conventional telecommunications companies and Internet access providers. European fundamental rights law adopts a broader view. In the functional conceptualization of ‘communications’ adopted in fundamental rights law, ‘communications’ is a dynamic concept, explicitly open to including new technologies that infringe on fundamental rights. In Part I and Part II, these respective conceptualizations are extensively studied.

‘Should’ points at the normative character of the study. Based upon descriptive legal research in chapters 2, 3 and 4, it is argued that a general positive human right to communications security is emerging from European fundamental rights law. As these fundamental rights requirements are being developed in response to recent cases, and many more future cases, coming before the courts, the study fills the current void by normatively arguing for a stricter stance on protecting private communications security by the EU lawmaker. The study offers a conceptual and legislative toolkit through which the legislature should further develop the new doctrine, leading to a general model for legislate communications security in EU law, tested in two case studies.
‘Protect’ is chosen as an element in the research question to examine the descriptive obligations and normative imperatives for states to actively protect communications security. Also, the research question excludes an analysis of the role of user empowerment, for example through education, as a viable strategy for protection. Based upon empirical and theoretical insights from behavioral economics, a wide range of studies in information law have emphasized the shortcomings of user empowerment in the field of online privacy and data protection and call for increased protection. In communications security, the fundamental shortcomings of user empowerment are even more pronounced as the average user cannot be expected to deal with complex technological trade-offs and policies that even programmers themselves often do not understand. Also, the study researches protection through legislation as a strategy for augmenting private communications security, rather than strategies of deterrence through criminal law and cyber warfare. Criminal and military law are only mentioned in passing when the mitigation of cybercrime and warfare leads to legal measures or intelligence or law enforcement agency conduct that perversely impacts the overall communications security enjoyed in the networked environment. As to cybercrime, only its conceptualization of ‘security’ in EU cybercrime law is analyzed in Part I.

1.2. Methodology and Limitations

This is a study in information law, which “comprises a wide set of legal issues at the crossroads of intellectual property, media law, telecommunications law,

---

37 The protection and empowerment strategies are inspired by Zuiderveen Borgesius 2014.
38 See extensively Zuiderveen Borgesius 2014.
39 Whitten & Tygar 1999.
freedom of expression and right to privacy.”

Positioning the emerging field of communications security law within information law is one of the core research goals of the study. The historical analysis of EU communications security law in Part I (especially sections 2.1-2.6), first sections of the constitutional analysis in chapter 4 and the sections on EU law in the case studies of Part III are descriptive and thus identify ‘what the law is’. The last two sections of chapter 4, the conclusions of Part III and the proposed regulatory model of Part IV can be characterized as mainly ‘normative’ legal scholarship, or ‘what the law ought to be’.

The legal research methods of this study are primarily desk research and literature review. Primary legal sources, legislative history, case law, soft law and legal literature are reviewed, along with internationally recognized technological standards. The study generally adopts an internal viewpoint, although to some extent it could be described as a study in law and technology.

This study can be characterized as pragmatic legal research that aims to arrive at recommendations, both theoretical and practical, for the EU lawmaker. Its arguments and recommendations are thus tailored to the internal logic of the European legal system. To a certain extent, the study also questions the desirability of the EU as a lawmaker in the political perspectives of chapter 6 and beyond.

As case law and legal literature are quite scarce, the conceptual analysis of part II draws inspiration from computer science, security economics, political

42 Koops 2013.
science, international relations and surveillance studies literature. Parts I and II present the results of these research efforts. Substantial parts have been presented at academic and policy conferences and talk series. The legal-historical and conceptual analysis of Parts I and II have served as a foundation for the design of a regulatory model for EU communications security law.

The regulatory model proposed by this study was subsequently operationalized in two case studies, on HTTPS and ‘cloud’ communications breached by operation MUSCULAR, as revealed by Edward Snowden. The cases have been selected to complement one another: HTTPS covers the user-provider relationship in web browsing, while the ‘cloud’ communications targeted in operation MUSCULAR affect so-called interdomain communications (between providers) and intradomain communications (within the network of one provider). Jointly, the case studies cover the functional value chain of web-based communications along a functional value chain, while the associated communications security breaches have affected millions of citizens for an extended period of time. As such, the case studies can serve to further examine and specify the conceptual framework and regulatory model offered by this study. In addition, the studies contain original security economics and computer science research, conducted jointly with scholars trained in these disciplines. A significant part of the case studies has been peer-reviewed, presented and published in leading conferences and journals. These publications have been complemented in this study, in particular with the positive fundamental rights obligations on legislating communications security. The case studies add insights for scholars across disciplines. In that sense, the study could be characterized as inter-disciplinary. But the emphasis of the

---

44 See, for example, Arnbak 2013.
entire study is on contributing to an emerging subfield of information law, i.e. communications security law.

The research questions and results were discussed during an international workshop specifically organized on this study, held at Harvard University’s Berkman Center for Internet & Society on 18 April 2014.46 The workshop brought together academics, advocates and hackers that work in the spheres of information law, policymaking, computer science, economics, philosophy and political science. A second workshop was organized to explore the technical dimensions of communications security at the Institute for Information Law.47 Funding was provided by the Institute for Information Law, the Berkman Center, Foundation Democracy & Media and Stichting Internet4ALL. Apart from the conferencing and publication of papers, preliminary results were reviewed by and debates held with experts from various disciplines and sectors from across the world. The research for the thesis as a whole was concluded on 1 July 2015, with minor updates across the thesis until 5 September 2015.

Limitations

As one of the first doctoral projects in EU communications security law, the limitations of the study are considerable. The topic is always ‘on the move’. While historical analysis does not ‘run away’, some of the analysis based on descriptive observations may be outdated soon after the publication of the thesis. After a decade of relative calm, the EU has initiated legislative programs in all five subfields of EU communications security law. The European fundamental rights courts are set to rule on a number of seminal cases in the upcoming years. The Snowden revelations are still ongoing, and will probably

46 Program, participants and references see: <https://pad.berkman.harvard.edu/comseroundtable>, accessed 1 September 2015.
continue for another year. Security economics market analyses need constant updating and verification.

The study sometimes feels like a mile long but only an inch deep, as it surveys these different perspectives relevant to communications security. Aware of these inherent limitations, the study has sought to cope with them through joint authorship, peer-review, conferencing and research fellowships. The rapid development of the research topic was addressed by taking a step back from too specific analysis of one particular legal instrument. Instead, the thesis conducts conceptual research through fundamental rights, systems design and political perspectives. As the study constitutes one of the first multi-disciplinary studies to appear in the academic literature on EU communications security law, it aspires to become a first point of discussion and reference and for formulating new research questions, rather than a definitive textbook on EU communications security law.

1.3. Scope

Within the research question, a number of relevant research directions could not be pursued in this study. With regard to legal research, the role of EU law and the strategy of protection are central elements of the research question. National and international law (such as U.N. policymaking) are only mentioned in passing to provide context. The study does not conduct external comparative legal analysis, for example by comprehensively comparing the EU to US legislation. The conventional legal strategies of lawful access, cyber warfare and new investigative powers – such as the controversial proposals for and practices of hacking by law enforcement agencies – are quite hotly debated topics currently, but not within the scope of this study. Prior work has
addressed such issues extensively.\footnote{Arnbak 2009. Van Hoboken, Arnbak & Van Eijk 2012. Arnbak 2014a,b,c. Arnbak 2013.} This study does not engage with military law or penal law, only insofar these areas provide input for the conceptualization of ‘security’. Simply put, the study is about defense, not offense. In fundamental rights parlance, the study is more about the foundations and legislative tools for protection, and thus establishing the essence of rights, rather than the limitations on their enjoyment. Obviously, the notions of right and limitation interact with one another, and the interaction is treated across the study. The newly established positive obligations to technical security are extensively discussed in chapter 4. Then again, one critical area that will surely develop considerably over the next decade is the place of communications security vis-à-vis the new ‘freedom to conduct a business’ of article 15 EU Charter. As of yet, little case law or legal literature is available to meaningfully assess its role in the near future.

The study is not a full account of the Snowden revelations, nor a systematic overview of all relevant European fundamental rights case law. The study cannot give a full account of relevant regulatory theories on EU legislative rulemaking, nor is it a detailed treatment of data protection, telecommunications law or one of the other policy cycles identified in the historical analysis of chapter 2.

Since the turn of the millennium, many scientific disciplines have started to engage with the technical conception of computer security. This study focuses on the fundamental rights and market economics of technical security. Within these market developments, the study does not consider platform openness,\footnote{Zittrain 2008.} but rather the incentives of communications providers to produce communications security. The study is not about the psychology or behavioral economics of security. The user perspective adopted departs from the
observation that users, even less so than in data protection, cannot reasonably be expected to have the expertise, time and awareness to make rational choices on protecting themselves and optimal interests. Privacy Enhancing Technologies (‘PETs’) will only be briefly mentioned from the perspective of affording user protection through law, and will not be studied for their practical utility nor their technical merits. Finally, chapter 6 surveys political science literature to provide more insight into the political conception of security and its implications for EU lawmaking. But a general political science or more specific securitization analysis of EU communications security legislation is beyond the scope of this study.

1.4. Outline

Part I of the study contains a historical analysis of EU communications security legislation. Describing definitions, scope and central provisions of five newly identified ‘policy cycles’, it presents the first comprehensive overview in the legal literature of the current European regulatory framework known to the author. The historical analysis formed the analytical framework (chapter 3) for the research throughout the study.

Part II provides a legislative conceptualization of ‘communications security’ from a fundamental rights (chapter 4), systems design (chapter 5) and political perspective (chapter 6). The fundamental rights chapter develops the positive human rights obligations to ensure communications security through EU legislation. The systems design chapter also addresses why systems fail, distinguishing between user, technical, market and surveillance failures. The

50 See, comprehensively, Zuiderveen Borgesius 2014.
51 Diaz, Tene & Gürses 2013.
political science chapter explores the political conception of security and the political dynamics of protecting communications security through EU law.

Part III uses the conceptual framework and tools as foundations for developing a step-by-step regulatory model for analyzing if the EU lawmaker should protect private communications security. The model is deployed in two case studies, into widely used communications technologies: HTTPS and the ‘cloud’. While substantial parts of these case studies have already been peer-reviewed or presented at leading conferences, they contain new material on the conceptualization of security, fundamental rights analyses, and technical solutions and proposed or adopted legislation by the EU.

Finally, Part IV analyzes how the EU lawmaker should protect private communications security and presents the conclusion of the entire study. Here, the study answers the central research question, offers five broad recommendations to the EU lawmaker and gives some directions for future research. Finally, the study sketches the outlook of EU communications security law on the short and longer term.
PART I: A HISTORY OF EU COMMUNICATIONS SECURITY LAW

2. Five EU Communications Security ‘Policy Cycles’

Regulatory failure can often be attributed to shortcomings in legal definitions. The apparent lack of a comprehensive overview of the EU regulatory framework of communications security is not a good omen in this respect. A 2013 policy study commissioned by the European Parliament calls the exercise of providing such an overview ‘undoubtedly highly complex’, and in the end dodges the question at hand. This chapter seeks to fill the gap, as it maps over three decades of information and communications security conceptualizations in E.E.C., E.C. and EU policies, sketching the relevant regulatory framework of EU communications security law in the process.

Sections 2.1 to 2.6 identify five communications security policy cycles, and offer what appears to be one of the first attempts of a comprehensive description of EU communications security law. Spanning roughly four decades, the historical analysis shows that communications security regulation is nothing new, and that mapping the past proves critical in understanding current conceptualizations of ‘security’ and the underlying dynamic and interests in current policies: in all the identified subareas of communications security policymaking, new legislative proposals have been proposed and, some even adopted in 2013. These proposals are set to influence global Internet governance.

53 Baldwin et al. 2011, p.68.
55 Eg. N. Robinson et al. 2013.
A holistic evaluation of these communications security policies is conducted in section 2.2, which subsequently develops six research themes on the intersection of computer science, political theory and legal studies. From the evaluation, a research agenda is developed on how to conceptualize and regulate communications security. This research agenda sets out the analytical framework of Part II of the thesis.

The five policy cycles that can be distinguished are: network and information security, data protection, telecommunications, digital signatures and certificates, and cybercrime. The areas are presented more or less chronologically in terms of legislation adopted. A US readership might wonder why ‘national security’ is omitted as a policy cycle. The EU Treaties explicitly exclude ‘national security from EU competence:

“[The EU] shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State”

As such, ‘national security’ is a sole responsibility of EU Member States, and not a separate EU policy cycle. It will become clear that this often overlooked fact, most notably in the wake of the first Snowden revelations, puts its mark on any effort to secure communications through EU regulation. Notably, the federal structure of the US works exactly opposite; in the sense that national security is not dealt with at the state level, but rather ‘a sole responsibility’ of the federal government, particularly the Executive Authority.

The sub-sections mostly overlap with these five policy cycles, apart from sections 2.1 and 2.6 that are later merged into the ‘network and information

57 Arnbak & Goldberg 2015.
security’ cycle. Each section starts with providing the historical context of the policy cycle: the first instruments adopted, the policy rationales for doing so, and a short description of some of the prominent provisions throughout the years. At the heart of the analysis of these policy cycle lies a description of the definitions of ‘security’ and their scope. Scope is understood as the policy area a particular instrument covers, which often means what providers are subject to regulation, and what the rationale is for the regulatory instrument – securing information or networks, or if other interests have prevailed (such as national security or market structuring).

The definitions of ‘security’ that are mentioned in the legal instruments are analyzed against the well-known and broadly acknowledged “c.i.a.-triad” in computer science. In the Encyclopedia of Computer Science, Pfleeger defines them as follows:

- **Confidentiality** – assurance that data, programs, and other system resources are protected against disclosure to unauthorized persons, programs, or systems;
- **Integrity** – assurance that data, programs, and other system resources are protected against malicious or inadvertent modification or destruction by unauthorized persons, programs, or systems;
- **Availability** – assurance that use of data, programs, and other system resources will not be denied to authorized persons, programs, or systems.

In computer science, a rich literature further specifies and interprets the confidentiality, integrity and availability triad (the ‘c.i.a.-triad’), elements referred to as security goals. It begs the question to what extent, in all those decades, policymakers have appreciated the insights from computer science,

---

59 See section 5.1.
and how policies may, or may not have come to a clear grasp of how to translate these security goals into sensible policies.

The year 2013 saw legislative action in all five areas identified, either with proposals or legislation adopted. A separate section 2.6 is devoted to the ‘Network and Information Security’ Directive, proposed by the European Commission in February 2013 and currently debated by the EU Parliament and the EU Council of Ministers – the institution in which national governments find their EU seat. This new proposal speaks to all the policy cycles identified, and will give an actual indication of the ambitions of the EU institutions to augment private communications security. A political confrontation of EU institutions in 1990 is highly instructive in forecasting the outcome of that process.

2.1. Information Systems & Critical Infrastructures

The ambition of EU institutions to treat the security of ‘information systems’ as a separate policy area traces back, at least, to a 1992 Council Decision ‘In the Field of Information Systems’. The issue statement of the 1992 Decision reads like any opening statement of a policy document today:

“1.1. Issue - security of information systems is recognized as a pervasive quality necessary in modern society. Electronic information services need a secure telecommunications infrastructure, secure hard- and software as well as secure usage and management. An overall strategy, considering all aspects of security of information systems, needs to be established, avoiding a fragmented approach. Any strategy for the security of information processed in an electronic form must reflect the wish of any society to operate effectively yet protect itself in a rapidly changing world.”

---

The issue statement of the 1992 Council Decision observes that coordinated action at the EU level is the needed to avoid ‘a fragmented approach’. That aim would not exactly be realized, as we will see. The final 1992 Council Decision contains little substance, but its legislative history is a fascinating moment in communications security policymaking for its underlying institutional politics.

A 1990 proposal of the European Commission and several European Parliament resolutions preceded the 1992 Council Decision. In 1990, the Commission proposal expressed broad ambitions for information security policies at the EU level. Its preambles gave considerable responsibilities to the European Commission, evoked the subsidiarity principle for EU action and mentioned that international coordination was necessary. A prominent justification read that information and communications security was not bound by traditional territorial notions of nation states. The document listed a broad set of underlying values for policymaking, such as ‘protecting privacy, intellectual property, commercial confidentiality and national security’.

In the Council text, however, such ambitions are toned down considerably. The document singles out facilitating a competitive business environment as the primary competence of EU level action in this area; information security should protect ‘business applications, intellectual property and confidentiality’. Other considerable changes in the Council Decision include the removal of the subsidiarity principle from the preambles; more representation of Member States in the expert group; the final say of the Council in cases of conflict, and the right of the Council to postpone actions suggested by the Commission (article 8 Council Decision). The Council,

---

61 COM(90) 314 final, OJ C 277/18, 5 Nov. 1990, p.18.
62 COM(90) 314 final, Annex, Action line II, article 2.1.7.
64 The Commission proposal merely obliged the Commission to send a report of its actions to other EU institutions (article 5 Commission proposal).
moreover, exactly determined the allocation of a tiny budget for European activities (2 million ECU per year, article 3 Council Decision). Excluding end user interest from the domain of critical infrastructure protection may have obscured the issue for other EU institutions, notably the European Parliament, in decades to come. The EEC Treaties in the 1990s did not prevent more ambitious approaches to augment the information and communications security of critical infrastructures to enhance public interests such as information and communications confidentiality or availability – similar to data protection or telecommunications provision. With the 1992 Council Decision, Member States claimed control of network and information security policymaking.

The legislation on the tasks of the European Network and Information Security Agency (‘ENISA’) shows how the institutional dynamic of the 1990s at the EU level still drives policymaking today. Article 1[1] of the 2013 ENISA Regulation states that its task is to “raise awareness and promote a culture of network and information security (…) for the establishment and proper functioning of the internal market.” Raising awareness and promoting a sense of urgency does not automatically give an institution actual authority. Among its other tasks are to support and contribute to voluntary efforts of other stakeholders (article 3), without any explicit mandate of enforcement. Furthermore, national security and criminal law are explicitly excluded from its mandate in article 1[2], even though criminal law falls squarely within the competence of EU lawmaking since the 2009 adoption of the EU Treaty of Lisbon. The internal market focus, voluntary nature of ENISA policies and exclusion of criminal law strike as familiar to the 1992 Council Decision

65 Contrasting with budgetary discretionary for the Commission as proposed by the Commission (article 3 Commission proposal).
discussed above. Indeed, ENISA’s impact has been analyzed as limited to providing ‘policy advice’, with a “poor uptake” of its reports.\(^{68}\)

Since the early 1990s, EU member states have made sure information and communications security policymaking is primarily regulated on the national level. As we will see, this dynamic is indirectly challenged in several other policy cycles discussed throughout this chapter. And the current institutional power structure is challenged again, directly, with the 2013 Commission proposal for a ‘Network and Information Security’ Directive (section 2.6.).

**Definition**

‘Security’ is not defined in the 1992 Council Decision. Article 1 in conjunction with article 2 call for the creation of an expert Committee (‘Senior Officials Group’) and contains calls for the development of action plans following six themes\(^{69}\) that are further outlined in an Annex and mostly describe a course of procedural action rather than relevant substantive details.

The first definition of ‘security’ in this policy cycle can be traced back to a 2001 Commission Communication.\(^{70}\) That 2001 definition has seen only slight modification over the years and is most recently codified in the 2013 ENISA regulation article 1[3]:\(^{71}\)

---

\(^{68}\) N. Robinson et al. 2013, p. 84.

\(^{69}\) Outlined in article 2[2]: “development of an information security strategy framework; identification of user and service provider requirements for the security of information systems; solutions for immediate and interim needs of users, suppliers and service providers; specifications, standardization and verification of information security; technological and operational developments for information security within a general strategy; provision of security of information systems.”


\(^{71}\) Regulation 526/2013, OJ L 165/41. The slight modification is the inclusion of ‘unlawful’.
'network and information security' means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems.

The definition seems directly inspired by the c.i.a. triad, but adds ‘authenticity’ to it. Unfortunately, additional argumentation or source material on why and how the Commission came to this definition is not provided. Subsequent EU documents that refer to this definition also lack further argumentation or source material.\(^{72}\) Apparently, those later definitions have simply been copied from the 2001 definition. ENISA may have produced several reports and organized a range of workshops, but their outputs are hardly distributed and do not have any binding force. The lack of guidance as to the meaning or intentions of the lawmaker is a cause of legal uncertainty and calls for further scrutiny.\(^{73}\)

**Scope: ‘Network and Information Systems’**

The 1992 Council Decision does not determine which entities are regulated. The 2013 ENISA Regulation offers only a reference to an incomplete description of ‘network and information systems’ in a 2006 Commission Communication.\(^{74}\) That document is vague across the board; it also proposes policy action “based on dialogue, partnership and empowerment” with “all stakeholders involved”.\(^{75}\) Such statements hardly provide guidance as to the scope of the instrument.

---


\(^{73}\) See section 1.2.

\(^{74}\) The 2001 Communication contains an imprecise description of networks, ‘systems on which data are stored, processed and through which they circulate’ and an unfinished (!) sentence on applications and terminal equipment directly after it. COM(2006) 251 final, p. 9.

\(^{75}\) “The Commission proposes a dynamic and integrated approach that involves all stakeholders and is based on dialogue, partnership and empowerment (…) in an open and inclusive multi-stakeholder dialogue.” COM(2006) 150 final, p. 6.
A 2001 Communication does mention that “all events that threaten security need to be covered”, and provides an “overview of threats.” The examples are quite detailed and mostly still relevant, such as failure by websites to implement browsing over HTTPS, network disruption discussing DDoS attacks and malicious representation discussing identity fraud. The threats mentioned overlap with then already existing EU legislation in the areas of encryption, telecommunications and data protection. In 2013, an ENISA Regulation would state that ENISA may only support, but not interfere, with telecommunications and data protection regimes and supervisory authorities. Other threats mentioned in the Communication, such as the Echelon spying infrastructure, may fall within the definition of ‘network and information security’, but as subject matter national security is exempted from the policy cycle in article 1[2] ENISA Regulation.

Scope: ‘Critical (Information) Infrastructures’

In 2005, the American political concepts of ‘critical infrastructures’ and ‘cybersecurity’ enter the EU policy arena. A Green Paper drafted by the Commission, upon the request of the Council, eventually leads to the 2008 ‘Council Directive on European Critical Infrastructures’. Again, the Council assumes control of the policy area and deems critical infrastructure protection primarily as an issue of Member States’ national security (recital 4).

Apart from identifying new European Critical Infrastructures (‘ECI’) in the energy and transport sectors (Annex I), the Council Decision lays out a procedure to possible identify other sectors (Annex III). With regard to ICT,
the Council considers but does not identify the ICT sector as a Critical Infrastructure in the 2008 Decision (recital 5). The consequence of being deemed an ECI is that operators in those industries should have a security plan (article 5 in conjunction with Annex II) and a liaison officer for communication purposes (article 6) in place, but it is up to Member States to determine most of the details and to enforce such obligations.

Adding to the confusion, in 2009 the Commission introduced a sub-class of Critical Infrastructures with regard to ICTs – so-called ‘Critical Information Infrastructures’. Including Internet backbone providers in its scope, this strand of policy is primarily concerned with encouraging the availability (or continuity) of communications through a host of newly erected voluntary public-private partnerships. 81 Both in critical infrastructure and critical information infrastructure policymaking, the voluntary nature of the regulatory measures is emphasized, and a sprawling web of organizations and working groups has emerged. That dynamic has been accelerating ever since, as recently new ones are being introduced on a seemingly monthly basis. 82

Overall, policymaking in this field has not achieved in offering a clear picture of what ‘network and information security’ entails, nor what stakeholders fall within its reach. Meanwhile, policies often refer to several other cycles of EU policymaking. Indirectly, those other avenues of policy have had much more actual impact on the conceptualization of ‘security’ at the EU level. A close study of these related and often overlapping policy cycles is needed to comprehensively analyze the 2013 Commission proposal for a ‘Network and Information Security’ Directive (section 2.6.).

82 N. Robinson et al. 2013, p. 80 and reiterated by the authors on p. 96, report IP/A/ITRE/NT/2013-5 PE 507.476 to the ITRE Committee of the European Parliament.
2.2. Data Protection

Since the inception of data protection, the security of personal data has been around as a concept. Under different definitions, each increasingly elaborate, data security was part of the earliest versions of the Fair Information Practice principles in 1973, the US Privacy Act of 1974, the OECD Fair Information Practice Principles, and made it into the influential 1981 Council of Europe Convention no. 108. That convention provides the basis for the 1995 EU Data Protection Directive, with its provision on ‘data security’ in article 17. That provision is still considered one of the cornerstones of EU ‘security’ legislation and enforcement today.

Definition

Many EU legislative instruments follow the wording of the Data Protection Directive, which defines ‘security of processing’ in article 17(1):

‘Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.’

85 US Privacy Act of 1974, 5 USC Sec. 552a(e)(10).
88 Section VIII of the Data Protection Directive contains article 17 and is titled: ‘the confidentiality and security of processing’, which in itself reveals that the c.i.a.-triad has not been followed.
The first part of the definition closely follows article 7 of the CoE Convention no. 108, but then the provision specifically adds a sentence on networked transmission on top of the original convention. That first part mirrors the c.i.a. triad, as disclosure or access appeal to confidentiality, alteration to integrity and destruction or loss to availability. It is a bit narrower than the c.i.a. triad, as it does not cover temporary loss of data availability. Ensuring data availability in tense situations such as emergency healthcare is as such not covered by the Data Protection Directive. In more recent opinions, the Article 29 Working Party has started to explicitly employ the c.i.a.-triad.

The second part of the definition reveals that the provision may touch on both information and network security, given the addition of ‘in particular where the processing involves the transmission of data over a network’ to article 17 Data Protection Directive. Recital 47 of the Directive explains that telecommunications or electronic mail service providers are deemed controllers for the traffic data generated by using those services. The 1997 predecessor of the E-Privacy Directive would further elaborate on these observations.

The provision today still refers to network security, and there has been some action in this particular area by data protection authorities. The Dutch Data Protection Agency, for instance, started enforcement actions in July 2013 against 43 private doctors for not providing HTTPS-encrypted web communications to end users for forms on their websites. The enforcement

---

90 See, for example, Article 29 Working Party 2012, WP 196.
91 See section 2.3.
92 CBP, Onderzoek naar de beveiliging van het online aanvragen van herhaalrecepten bij huisarts en apotheek, May 2013, p. 3.
action was based on a sector specific standard\textsuperscript{93} that finds its legal base in the Dutch implementation of article 17 of the Directive, article 13 of the Dutch Data Protection Act. Curiously, article 13 of the Dutch Act has removed the network security sentence from its provision. Nonetheless, a communications security enforcement action is taken by the data protection enforcer, when communications or data security are seen as interdependent. Such enforcement actions point to an uncertain and complex legal relationship between communications and data security.\textsuperscript{94}

\textit{Scope}

The 1995 Directive’s ‘security’ provision is only applicable to organizations that control or process ‘personal data’\textsuperscript{95} – a key term in the Directive that captures those data that can directly or indirectly lead to the identification of a person.\textsuperscript{96} The scope of ‘personal data’ has been expanding ever since the adoption of the Directive in 1995 and remains the subject of intense political and academic debate ever since.\textsuperscript{97} But, as observed before with article 17 of the Directive, Courts and Data Protection Authorities often interpret the term in light of new technological realities. For instance, IP-addresses are usually considered to be personal data. Regardless, certainly not all information and

\textsuperscript{93} NEN 7512:2005, \textit{Medische informatica - Informatiebeveiliging in de zorg - Vertrouwensbasis voor gegevensuitwisseling}, p.15.

\textsuperscript{94} See sections 2.7 and 3.1.

\textsuperscript{95} Both ‘controllers’ (article 17[1]) and organizations that ‘process’ personal data on their behalf (article 17[2-4]) are covered in the Data Protection Directive. In outsourcing, for example, data security must be ensured through a private contract that assures a similar level of protection demanded from the ‘controller’ in article 17[1] DPD.

\textsuperscript{96} Defined in article 2(a) Directive 95/46/EC: ‘any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity’.

communications constitute ‘personal data’. Corporate information, draft government policies or media reports stored on some server in the cloud do not necessarily contain personal data, for example.

The simple observation that data protection policy only covers ‘personal data’ is often overlooked, for instance in the initial European response to the Snowden revelations. Policymakers took to data protection, notable its safe harbor regime on international data transfers, for solving legal issues around ubiquitous surveillance including communications security. But national security falls outside the material scope of data protection regulation for reasons of EU competence – national security is up to the Member States individually. And due to its definitions and scope, data protection as a solution is inherently limited when addressing a plethora of vexing legal issues. Only a small subset of the data in which intelligence agencies may be interested will be covered by data protection in the first place.

Recent Legislative Action

The 1995 Directive is currently under review after the Commission proposed a Regulation in January 2012. The proposed General Data Protection Regulation (‘GDPR’), if adopted, acquires immediate binding force across the EU without a need for implementation on the Member State level. The long awaited and quite massive legislative effort has led to a record amount of amendments filed with the European Parliament, but in March 2014 the Parliament nearly unanimously adopted a comprehensive legislative package. While the

98 Zuiderveen Borgesius 2014.
incoming Greek EU Council Presidency had given priority to data protection, for various reasons – the German government reluctant to lower standards, the UK defending business interests – the Member States in the EU Council agreed at an October 2013 summit to move the deadline for adoption until 2015. With the heads of government openly debating data protection in the media, and amidst ongoing revelations on transnational intelligence gathering by all governments involved, data protection has become even more politicized than it already was when the Commission launched its initial proposal in 2012. Therefore, the implications of the entire process for the current arrangements around article 17 are hard to assess at this point.

2.3. The Telecoms Package

The European regulatory framework for electronic communications originates in a long legacy of state-owned postal and telecommunications companies. The 1990 legislative package now known as the ‘Open Network Provisions’ aimed to liberalize the telecommunications market. Today still, the main aim of the Telecoms Package, in the words of the European Commission, is ‘to strengthen competition by making market entry easier and by stimulating investment in the sector.’ This legacy has real consequences for its security provisions, as we will see.

The 1997 ‘Telecommunications Data Protection and Privacy’ Directive contained a general communications confidentiality requirement in article 5. Interestingly, the European Commission originally included a specific and robust network security requirement in its proposal for the Directive of 1990. Article 8[2] of that proposal contained an explicit obligation for end-to-end encryption in telecommunications networks. The end-to-end encryption proposal never made it into the final 1997 Directive. Today, many call for legal safeguards for strong end-to-end encryption in response to the Snowden revelations. Contemporary advocates of end-to-end encryption are probably unaware of those legislative debates on crypto in the Telecoms Package, already taking place over two decades ago against the background of liberalization of telecommunications. It is unclear why end-to-end encryption did not make it into the Directive. The explanation might lie in a combination of the priority of market liberalization and competition law over privacy, at a time when the crypto wars were waged primarily in the encryption policy cycle (see section 2.4).

The current relevant provisions can be found in the 2002 Framework and E-Privacy Directives, respectively both amended in 2009. Article 5 of the E-Privacy Directive still contains the same general confidentiality obligation as in 1997. Notable communications security measures introduced with the 2009 amendments are risk-assessment based ‘security’ obligations and a security policy with regard to personal data processing, ‘integrity’ obligations to

---

protect continuity, a ‘security’ breach notification and a personal data security breach notification.

**Definition**

The 1990 Open Network Provisions included the ‘Commission Liberalisation Directive’. It contains provisions on ‘security’ and ‘integrity’ in recital 9 that already point at underlying concerns at the time:

“(9) the security of network operations means ensuring the availability of the public network in case of emergency. The technical integrity of the public network means ensuring its normal operation and the interconnection of public networks in the Community on the basis of common technical specifications. The concept of interoperability of services means complying with such technical specifications introduced to increase the provision of services and the choice available to users. Data protection means measures taken to warrant the confidentiality of communications and the protection of personal data.”

While introducing security measures, ‘security’ itself is not defined in that Directive. The c.i.a. triad remains not followed in its entirety until today. The definition of ‘security’ in 1990 emphasizes availability and interconnection, which points at liberalization of state monopolies and creating conditions for market entry as driving forces of the legislation. Data protection is subsequently seen as confidentiality of communications and data. Integrity is framed as ‘normal operation’, not at all the same as the definition of integrity in computer science literature.

---

112 Article 6 jo. article 1 jo. rec. 9 Directive 1990/388/EC (‘Commission Liberalization Directive’).
Over time, the conceptualization of ‘security’ in the 1990 Commission proposal and 1997 Directive would lead to confusing situations in the current Directives of the Telecoms Package. The confusion plays out on at least three levels. First, confidentiality enjoys broad protection under article 5 E-Privacy Directive, which mentions both confidentiality of “communication” and “information”. The E-Privacy Directive also mentions the ECHR and the Charter of Fundamental Rights of the EU in its opening recitals 2 and 3, as well as 24. For the other security attributes, article 4 of the E-Privacy Directive implies that security is only of concern when personal data is involved.  

Second, the Telecoms Package contains a general ‘networks and services’ security provision (article 13a[1]) and a separate obligation for regulated entities to ensure the integrity of their networks (article 13a[2]). Had the Directives followed the more comprehensive definition of ‘security’ of the c.i.a. triad, article 13a[1] would be more comprehensive and less confusing, while article 13a[2] would have been superfluous. Thirdly, the integrity provision of article 13a[2] ensures ‘continuity of supply of services’. But that concerns availability, rather than integrity. Taken together, the interplay between ‘security’ in article 13a[1] and integrity in article 13a[2] is unclear, and not specified in recitals. It remains an open question whether the c.i.a.-triad attributes of the communications that are covered within the Telecom Package are covered by the legislation. It is uncertain if, and how, communications integrity as defined under the c.i.a.-triad is covered.

The legal uncertainty is exacerbated by the fact that, across the board, the lawmaker delegates determination of the details to the European Commission

---


114 According to article 13a[1], Member States must ensure that regulated entities ‘prevent and minimize the impact of security incidents on users and interconnected networks’. Article 13a[2] rules that Member States ensure that regulated entities ‘guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks’.
in article 13a[4] Better Regulation Directive. The provision directs the Commission to follow ‘international standards to the greatest extent possible’, even though the provisions themselves do not align with international standards on such basic issues as terminology. International industry standards usually follow the c.i.a.-triad.

Furthermore, entrusting communications security to industrial standard setting procedures does not automatically yield optimal outcomes from a communications security perspective. It has been known for a long time among security experts that the GSM encryption standard A5 had been deliberately weakened through pressure by intelligence agencies.\textsuperscript{115} This take on history has recently been confirmed amidst the Snowden disclosures, when four Norwegian engineers that took part in creating the GSM-standard process in the early 80s finally dared to speak up to and provide the details of the story. They pointed at the UK government for leading the effort in choosing weaker keys (54-bit instead of 128-bit) to enable intelligence gathering.\textsuperscript{116} Strikingly, the weakened encryption standard adopted back then is still in wide use today, for instance in European 2G networks, leaving European mobile communications vulnerable to security breaches.\textsuperscript{117}

Such observations on standardization, as well as the failed attempt of the Commission to include end-to-end encryption as a security requirement in 1990

\textsuperscript{115} Anderson 2008, p. 615. In 1994, Anderson wrote a piece for UK Telecom, claiming that “there was a terrific row between the NATO signal intelligence agencies in the mid-1980s over whether GSM encryption should be strong or not. The Germans said it should be, as they shared a long border with the Warsaw Pact; but the other countries didn’t feel this way, and the algorithm as now fielded is a French design.” R. Anderson, *Hacking Digital Phones*, UK Telecom, 17 Jun. 1994.

\textsuperscript{116} See <http://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html>, accessed 2 September 2014.

and beyond, spur the question how to determine ‘acceptable’ levels of security in light of the general security obligations in article 13a Better Regulation Directive. One can have a solid confidentiality provision with article 5 E-Privacy Directive, but if the combination of article 13a Better Regulation Directive and standardization allows the maintaining of a vulnerable encryption protocol for GSM over decades, a powerful adversary can get backdoor access to those communications regardless of confidentiality provisions in place.

Scope

The scope of the Telecoms Package is largely limited to providers of ‘electronic communications networks’ and ‘electronic communications services.’ Here, the market structuring legacy of the 1990 Open Network Provisions manifests itself directly. On the face of it, only conventional telecommunications and Internet access providers fall within the scope of the Telecoms Package, being the ‘transporteur’ of communications primarily in the business of signals transmission. Other communications providers, such as information society services (think social network services and webmail providers), seem to fall outside its scope. On the face of it, the Telecoms Package fails to appreciate crucial socio-technical developments in electronic communications since the 1990s, such as digitization and the convergence of

---

118 The cookie and spam provisions in the E-Privacy Directive regulate a broader set of relevant stakeholders, according to article 5 and article 13. Article 29 Working Party 2009, WP 159, par. 2.1, note 7. See also Zuiderveen Borgesius 2011, p. 211.
119 See article 2[a] in conjunction with 2[c] Directive 2009/140/EC. Networks that fall within the scope of the definition in article 2[a] are those “resources which permit the conveyance of signals irrespective of the type of information conveyed”. Services are those “that consist wholly or mainly in the conveyance of signals on electronic communications networks, but exclude services providing content”;
120 Steenbruggen 2009.
communications. However, two examples provide a deeper understanding of that dominant view on the scope of the Telecoms Package: the regulation of i) data- and security breach notifications, and ii) Voice over IP (‘VoIP’) communications. The examples point at the underlying priorities of telecommunications regulation in Europe, how they are connected to the Open Network Provision legacy and how this affects security conceptualizations and policymaking.

The European Commission proposed a (personal) data- and security breach notification for electronic communications providers in 2007. From the viewpoint of communications security, the most relevant intermediaries today are the companies that create, store, process and monetize the data and infrastructure that the obligation seeks to protect – notably ‘information society services’. Today, these so-called ‘over the top services’ provide most of the relevant functionality in networked communications, where the conventional access provider merely connects its subscribers to the web. Following this reasoning, a majority in the European Parliament – with support from the Article 29 Working Party and the EDPS – sought to extend the data- and security breach notifications to information society service providers in 2008. However, the Commission argued that the legal definitions of the Telecoms Package constrained Parliament to pursue such an expansion in scope. Consequently, the notification measures remained in place, but only for conventional ‘electronic communications providers’. Hardly anyone noticed when the Commission provided the notification guidelines for these

---

123 A personal data breach in the context of the Telecoms Package is defined similar to article 17 Data Protection Directive in article 2[h] Citizen’s Rights Directive: “‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.’ The security provisions in article 7 of the Data Retention Directive (2006/24/EC) follow the same approach.
125 Zuiderveen Borgesuis 2011, p. 211.
conventional electronic communications providers on 24 June 2013. Meanwhile, ‘information society services’ have suffered a wide range of major security incidents – such as the leakage of millions of login credentials by e-mail newsletter provider Epsilon, Yahoo! and LinkedIn – leaving the communications security and personal data of millions of users exposed. In this example, the European lawmaker focused on the ‘actor’ rather than the function of the communication, and the Parliament saw itself constrained by the legislative definitions on scope in the Telecoms Package.

The second example, the regulation of VoIP, reveals a surprising contradiction. Following the Commission’s reasoning with regard to breach notifications, VoIP providers would be regulated as information society service providers – falling outside the scope of the Telecoms Package. Following this line of reasoning, when Alice calls Bob using a fixed landline, the Directives apply. And when Alice uses VoIP technology to contact Bob, the providers of that communication, and thus its security, will go unregulated. The policies, however, are very different. According to the Commission, VoIP providers can fall under different regulatory regimes, and consequently with different regulatory obligations for communications security. Here, the market with which the service competes is what matters. When a VoIP provider calls a phone number rather than a user account (say, SkypeOut rather than Skype-to-Skype) the Telecoms Package applies. But the average VoIP user that has the service installed on a smartphone and receives a call does not reasonably notice

---

126 See article 1 Commission Regulation 611/2013.
127 From 2009 until 2013, NGO Bits of Freedom has maintained a ‘Zwartboek Datalekken’, a list of data breaches, at: <https://www.bof.nl/category/zwartboek-datalekken/>, accessed 2 September 2015.
128 “VoIP providers can be classified as providers of publicly available electronic communications services (…). This is however not the case for VoIP services that offer machine-to-machine communications essentially only consisting of the provision of a product.” SWD/2013/032 final, Impact Assessment, see <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013SC0032:EN:NOT>, accessed 2 September 2015.
the difference between, say, SkypeOut and Skype-to-Skype. The user probably expects communications security provisions to apply to both, but the law does make the distinction based on market competition considerations.

The examples reveal that market considerations can stretch the scope of the Telecoms Package, but communications security considerations cannot. The market structuring legacy of the Telecoms Package informs a communications security policy where the economic fact that a software product competes with an ‘analogue’ service provider prevails, rather than the function of the communications. The E-Privacy Directive’s scope has been stretched with regard to cookies and spam;\textsuperscript{129} these provisions of the Telecoms Package target providers beyond conventional telecommunications and Internet access providers as well – such as websites and webhosting providers. In the Telecoms Package, communications security is approached on an ad hoc basis, in which market and political pressures prevail. A rigorous conceptualization of ‘security’ and its scope would inform an approach that would not leave substantial gaps in communications security protection for end users.

**Recent Legislative Action**

In September 2013, the European Commission proposed a Regulation amending several provisions of the 2002 and 2009 Directives.\textsuperscript{130} The proposal and the proposed amendments to it in the Parliament don’t affect the definitions, scope or the security provisions introduced in 2009. The aforementioned problems with regard to definitions and scope are not bound to be addressed anytime soon.

\textsuperscript{129} Article 5 and Article 13 E-Privacy Directive. Article 29 WP, WP159 2009, par. 2.1, note 7.

\textsuperscript{130} COM(2013) 627 final, 2013/0309 (COD), ‘laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent.”
2.4. Digital Signatures and Certificates

Roughly until 1980, intelligence agencies closely guarded the means of production and use of encryption. Outside military and intelligence uses but within nations, relatively weak encryption was made available to, for instance, state-owned or controlled telecommunications companies (see section 2.3) to provide a certain but low level of communications security. At the same time, strict restrictions on the export of encryption were (and remain) in place to control the spread of encryption across national borders. In this way, intelligence agencies such as the NSA and GCHQ had close control over the adoption of encryption, while remaining capable of accessing weakly encrypted communications for surveillance and intelligence operations. Since the 1980s, however, more robust encryption was discovered and produced in private industry, academic and cypherpunk communities. Eventually, robust encryption became available for the average computer user.

The democratization of encryption spurred a fierce public policy debate, popularly known as the ‘crypto wars’, on the regulation of encryption. Where civil liberties advocates and business saw encryption as a central tool in protecting communications security, human rights and business practices such as online banking and E-Commerce, national security and law enforcement agencies voiced concern about their ability to conduct communications surveillance. Mass adoption of electronic communications, open access to encryption tools such as PGP and SSL-certificates and the promise of E-Commerce intensified these debates in the mid ‘90s.

---

131 Koops 2013. Koops maps encryption policies in a wide range of jurisdictions around the world. The survey focuses on export controls, encryption mandates and decryption orders for law enforcement. The EU section seems updated until 2002.
133 Swire & Ahmad 2012.
In 1997, the European Commission adopted a Communication on its encryption policy when the debates on its regulation reached a boiling point. The Communication, titled ‘Towards A European Framework for Digital Signatures And Encryption’, favored mass adoption of encryption. Compared to the US position on encryption, Andrews observes that the Commission took a relatively ‘liberal approach’. Andrews attributes the relatively friendly Commission position in part to the existence of article 17 in the Data Protection Directive and the Telecoms Package, particularly article 5 of Directive 97/66/EC (later the E-Privacy Directive). In addition, Blanchette points to a strong but in the end unjustified belief among policymakers that electronic signature technology would change a centuries-old practice around the legal status of hand-signed paper documents.

The 1997 Communication set the stage for the 1999 eSignatures Directive, which provided a harmonized framework for the provision of digital signatures and certificates across the EU. However, the national governments in the European Council succeeded in curtailing the ambitions of the European Commission on legislation at the EU level, leaving important specifics to the Member States. Throughout the 1990s, the European national governments had been leaving ample room for weakening cryptography in public statements by government bodies. With the 1999 Directive – notably its omission of the prohibition for Trusted Service Providers to store private keys (discussed

---

135 COM(1997) 503 final, para. 2.2. In considering national security and law enforcement concerns, the Commission argued that regulating encryption would not stop targets of investigations from using it, signaling the attribution problem and steganography (information hiding) as tactics.
136 For a comprehensive overview of the debate, see Andrews 2000.
137 Andrews 2000, para. 5.2.
below) — the EU Council has achieved what it aimed for. This has led to enabling commerce to thrive by providing some integrity requirements and low regulatory burdens, but at the same time allowing for weak encryption and security requirements in EU legislation, both in the E-Signatures Directive, and in the E-Commerce Directive. Obviously, the Snowden revelations — particularly the BULLRUN operation aimed at weakening encryption standards, technologies and implementations — provide new perspectives on the regulation of encryption and role of intelligence agencies beyond the crypto wars of the 1990s.

Definition

‘Security’ is not defined in the eSignatures Directive. Article 8 mandates that the provision of security products must comply with data protection measures of the Data Protection Directive and the Telecoms Package. The Annexes to the Directive contain several security requirements for regulated entities that mostly appeal to the integrity attribute of the c.i.a. triad, and that apply to a small set of actors (see ‘scope’, below).

The omission of a definition has important consequences, which can be demonstrated by looking at one legislative development in the 90s. The 1997 Commission Proposal for the Directive prohibited private cryptographic keys to be stored by the trusted third parties that provide them, called Certificate


\[142\] See for example Levy 2001. The book title, How the Code Rebels Beat the Government Saving Privacy in the Digital Age, is interesting. Understandably enthusiastic at the time, the Snowden revelations have made clear that the book’s main thesis is over-optimistic and naïve. It may only hold up with regard to a very small subset of technologies such as PGP and TOR, employed by only a fraction of the user base across the internet.
Service Providers (‘CSPs’; generally known as Certificate Authorities, ‘CAs’). In the Council Common Position, however, and ultimately in the eSignatures Directive, this requirement was removed, ostensibly under fierce pressure from the UK and US Government.

The question of private key storage by the CAs is an essential part of any confidentiality and integrity assessment. Private keys need to remain private for encryption to work, since a compromise of a private key entails a fundamental breach of trust and security. It enables encrypted information to be intercepted or modified by a man-in-the-middle attacker. Arrangements for private key recovery – such as key escrow and the ‘Trusted Third Party’ construction – are designed to enable surveillance and intelligence gathering. At the same time, attackers beyond intelligence and law enforcement agencies can exploit weaknesses in such arrangements. A security definition in line with the c.i.a. triad could have spurred a more explicit political debate about the omission of such a critical prohibition, rather than have it tucked away in one of its Annexes.

**Scope**

The Directive applies to CAs in general, but the important provisions, such as the security requirements, only apply to those CAs that issue so-called ‘qualified certificates’. The original Commission proposal applied to all CAs, regardless of the type of certificate issued. But the scope was limited by the Council during its legislative process. The qualified certificates are a tiny

---

145 Arnbak & Van Eijk 2012.
146 Abelson et. al. 1998.
147 Defined in article 2[10] of the eSignatures Directive as: ‘a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II.’
subset of certificates issued, and used in specific contexts such as E-
Government communications. The Council added the ‘qualified certificate’
category to the Annex, with the effect that the vast majority of CAs, and the
vast majority of certificates issued in ordinary web browsing, do not have to
comply with the specific (weakened) security requirements.

Recent Legislative Action

The European Commission launched a revision of the 1999 eSignatures
Directive in June 2012, with a proposal for a Regulation on ‘Electronic
Identification and Trust Services’ (‘eID Regulation’). In the summer of 2014,
the final eIDAS Regulation was signed into law. Like the GDPR in data
protection, an eID Regulation would acquire immediate binding force across
the EU upon its adoption, without a need for implementation in the
legislation of Member States. The updates address various developments
since 1999. Generally, the use of encryption across electronic communications
has spread immensely, and today is seen as the minimum standard for
processing information in several vital sectors of the information society.
The deep security breach at Dutch CA DigiNotar in September 2011 has propelled
the update of the 1999 legislation, with considerable effort from the

148 COM/2012/0238 final, procedural file 2012/0146 (COD).
149 The US National Institute for Standards and Technology (NIST), on the other hand, is opting
for a multi-stakeholder solution and organizing a workshops aimed at non-regulatory policy and
technical resolutions to overcome the systemic vulnerabilities. See
150 Indeed, numerous Member States have expressed concern with the choice of the legal
instrument. As the instrument seeks to ensure a minimum level of security, and Member States
are free to ensure higher levels of security, these concerns will primarily reflect positions of
Member States that are concerned with high information and communications security levels,
quite similar to the Council debates in 1998. See EU Council, 17269/12, 7 Dec. 2012, p.7,
2012/0146 (COD).
151 For instance in the health sector, See CBP, Onderzoek naar de beveiliging van het online
aanvragen van herhaalrecepten bij huisarts en apotheek, May 2013, p. 3, at
<http://www.cbpweb.nl/downloads_raporten/rap_2013-beveiliging-online-
herhaalrecepten.pdf>, accessed 2 September 2015. The offering of HTTPS by default was
becoming the state of the art for leading internet companies on client-server connections, and has
received an impetus with the Snowden revelations.
Netherlands for legislative action at the EU level. The outcome of the review process is uncertain, but the Commission proposal can be analyzed.

The Commission proposal does not include a definition of ‘security’, nor does the finally adopted “Regulation on electronic identification and trust services for electronic transactions in the internal market” (‘eIDAS Regulation’). The one relevant connection to a conceptualization of ‘security’ is made in recital 11, where the instrument refers to the Data Protection Directive when regulated entities process personal data. Without a definition of security, the lawmaker again – as in the eSignatures Directive this replaces – does not give any guidance how the c.i.a. triad operates with regard to trust service providers, and how to balance competing interests.

As to its scope, qualified and general ‘trust service providers’ (including CAs) are to be regulated. The proposal contains general security requirements, a security breach notification and liability provisions for both types of trust service providers, with stricter security requirements for qualified trust service providers such as more rigorous authentication of clients. The technical and legal analysis of the accompanying documents is generally not convincing. The details of how trust service providers should assure communications security are to be determined by delegated acts of the European Commission. While the Commission includes both types of trust service providers, critical actors in encrypted communications, such as web browser vendors or website operators, are left untouched. Arguments in favor or against the policy choice are not provided, other than it is deemed ‘too complicated at this point.’

---

152 See Arnbak & Van Eijk 2012.
153 The Commission proposal is being considered by both the EU Parliament and the EU Council since June 2012, see 2012/0146(COD).
155 Of the original Commission proposal.
156 Arnbak & Van Eijk 2012.
157 A comprehensive analysis of the proposal can be found in: Asghari et. al. 2013.
the conclusion of the ordinary legislative procedure, the eIDAS Regulation was adopted in the summer of 2014. These most recent legislative developments are extensively discussed in the HTTPS case study of chapter 8, particularly section 8.6.

2.5. Cybercrime

A fifth area is the approximation of criminal law regarding security breaches. The history of cybercrime legislation provides useful insights into EU conceptualizations of communications security. It is one of the early avenues for policymakers in different institutional branches across a wide range of nation states – beyond Europe – to reach a seemingly broad consensus in the information and communications security policy area. Its definitions are copied in the proposed ‘Network and Information Security’ Directive (see section 2.6).

Much of today’s EU cybercrime legislation finds its substantial basis in the 2001 Council of Europe ‘Cybercrime Convention’. The Cybercrime Convention had been in preparation by an expert committee since 1996. Many national legal systems had already included ‘computer crimes’ in their penal codes in the 1980s, and a Convention of this kind had been envisioned at least since 1989. Until this day, the Convention enjoys a status as the widest adopted legislative treaty in this space. Several countries outside Europe have become a party to the Treaty, notably the US, Australia, Japan, and the United States. Russia and China have not, expressing concerns over sovereignty.

---

159 CDPC/103/211196.
161 Brown & Sommer 2011, p.85-86.
At the EU level, the 2005 Council Framework Decision on ‘attacks against information systems’ was updated in August 2013 with a Directive. Changes in the 2013 Directive include the implementation of ‘illegal interception’ from the Cybercrime Convention, increasing penalties for large-scale attacks (primarily aimed at deterring the spread of ‘botnets’) and impersonation and criminalizing the use of ‘tools’ that enabled attacks. The latter move has received much criticism from security researchers for criminalizing legitimate security research, such as penetration testing by security consultants as well as responsible disclosure by ethical hackers. To address legitimate uses of hacking tools, a direct intent requirement has been introduced in the Directive and further explained in recitals 16 and 17 of the final version. This intent requirement had already been part of article 6 of the Cybercrime Convention from its very outset.

**Definition**

The preambles and provisions in the Cybercrime Convention contain some of the earliest comprehensive conceptualizations of ‘security’. One of its central preambles reads:

“Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalization of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and

---

The c.i.a.-triad forms a central part of the preamble and the provisions of the Convention. Title 1 of Chapter II is named after it: “Offences against the confidentiality, integrity and availability of computer data and systems.” Articles 2-5 contain the substantial criminal law provisions on ‘illegal access’, ‘interception’ and both ‘data-’ and ‘system interference’. The explanatory memorandum makes clear that the provisions are directly linked to c.i.a.-triad theory,\textsuperscript{166} and drafted in a technologically-neutral way to ensure the durability of the Convention.\textsuperscript{167} In subsequent EU cybercrime legislation, however, the c.i.a.-triad would hardly be part of the legislative mindset. The c.i.a.-triad is not mentioned in the 2005 or 2013 legislation and explanatory documents. In addition, the explicit mention of botnets in the 2013 Directive provisions reveals a less technology-neutral mindset of the lawmaker.

As mentioned before, article 3 of the 2001 CoE Convention on the ‘interception of communications’ did not make it into the 2005 EU Cybercrime Directive; only into the 2013 version over a decade later. The interception article of the CoE Convention is one of the central provisions aimed at assuring confidentiality of communications of end users, and it had already been proposed in the 1989 Recommendation as deserving protection.\textsuperscript{168} Moreover, it was addressed in the 1997 case \textit{Halford v. The United Kingdom} before the European Court of Human Rights (‘ECtHR’) that concerned illegal wiretapping of an employee of the UK police by her employer.\textsuperscript{169} The explanatory memorandum of the Convention explicitly mentions \textit{Halford}, and further

\textsuperscript{166} CoE Cybercrime Convention, para. 43.
\textsuperscript{167} CoE Cybercrime Convention, para. 36.
\textsuperscript{169} ECtHR Halford v. United Kingdom 1997.
mentions five ECtHR cases to point at the fundamental rights dimension of the c.i.a.-triad and criminal law approximation in this space.170

In its 2002 proposal for a Council Decision implementing the Convention, the Commission copies several ‘threats to information systems’ from a Commission Communication in the ‘network and information systems’ cycle.171 ‘Interception’ is mentioned, but is considered to be dealt with in the Telecom Package.172 But that particular policy cycle only deals with conventional telecommunications providers, and is of a public law nature, not criminal law. Neither the Council nor the Parliament report further raised the issue.173 Later, in 2010, the Commission includes the provision without any further explanation in a proposal that would eventually become the 2013 EU Directive.174 Whether or not the criminalization of such actions is desirable, the public documentation of the EU institutions doesn’t even start to develop a vision on what it sought to criminalize in 2005, and why ‘interception’ was not part of it. An understanding of the c.i.a.-triad could have made the omission of the interception provision in the 2005 Directive, and its inclusion in 2013, a topic of public debate.

The Cybercrime Convention preamble names ‘deterrence’ as a main rationale for the instrument. ‘Deterrence’ aims at sending credible signals to possible adversaries that attack is futile, because it spurs serious retaliation. The

173 A5-0328/2002. The Parliament advocated a less strict regime, warned for the criminalization of legitimate actions, and amended the Commission Proposal to include fundamental rights safeguards across the text. The report was effectively neglected by the Council and in the adopted Decision. With the institutional structure of the time, the Parliament only needed to be consulted, rather than have the right to vote, with regard to matters of law enforcement policy in the Third Pillar of European Union policymaking.
doctrine has been inspired by game theory and international relations studies, and was of decisive influence in Cold War diplomacy and beyond.¹⁷⁵

The deterrence logic inherent in cybercrime policymaking may explain a puzzling prominence in the 2005 EU Council Decision of the threat of terrorist attacks on information systems, which apparently calls for strict cybercrime legislation at the EU level. But counterterrorism is the exclusive area of national security, and as such exempt from EU competence. Moreover, the effectiveness of counter-terrorism through deterrence in cybercrime legislation is contentious. In any event, it warrants further examination (see section 1.2.).

Conversely, the 2001 CoE Convention explanatory memorandum states that appropriate security measures themselves are “the most effective means” to prevent security breaches, rather than criminal law.¹⁷⁶ The 2013 EU Directive does the same in recitals 26-27, and even hints at imposing liability on providers that do not meet proportionate information security levels. Decades onwards in the cybercrime policy cycle, such comprehensive policy action has not materialized. The ‘Network and Information Security’ Directive proposed in 2013 aims to address this (see section 2.6.). The relationship between deterrence and actual effective network and information security policy deserves further attention (see section 1.2.).

**Scope**


¹⁷⁶ CoE Cybercrime Convention, para. 45.
The scope of the cybercrime policy cycle has been broad from the very outset. The Cybercrime Convention preamble, cited above, distinguishes a number of concepts that encapsulate the scope of cybercrime legislation. These concepts are further defined in article 1 of the Convention:

a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c) "service provider" means:
   i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
   ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

The definitions seek to capture any device, data or provider imaginable in the electronic environment. Devices can be both stand-alone machines as well as networked, in whatever form. The definition of service providers covers the entire range of providers: telecoms, information society services, and all other service providers conceivable in the electronic environment fall within the scope of the legislation. These definitions have not substantially changed over time, and are again part of the 2013 Directive. So along with a broad range of policy issues beyond communications security, comes the broadest set of regulated entities imaginable. In today’s information-mediated society, the cybercrime policy cycle thus encapsulates nearly everything, every time.

Apart from attacks against information systems, the measures also address actions “where computer and telecommunication systems are used as a means to attack certain legal interests.” These actions are outlined in articles 2-10 of the 2001 CoE Convention. Of note are the criminalization of child abuse and

177 CoE Cybercrime Convention, para. 36.
intellectual property infringements. In doing so, the Convention enable a possibility to conflate cybercrime with a wide range of other interests that are not directly related to the network and information ‘security’. This can be witnessed in the myriad of cybercrime and cybersecurity strategies seen across the EU in recent years.

2.6. The Proposed ‘Network and Information Security’ Directive


The Directive could be the first comprehensive legislative instrument in the broader area of ‘network and information security’. If adopted in the form the Commission proposed, the Directive would significantly break with the

178 The explanatory memorandum also points at ‘hate speech’, but notes that a consensus could not be reached because of freedom of expression concerns – hate speech was to be treated in an additional protocol to the Convention, which would be adopted in 2003. Council of Europe Convention on Cybercrime, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, CETS 189, Budapest 28 Jan. 2003, see <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>, accessed 2 September 2015.
179 See section 1.2.5.
voluntary and EU Council dominated approach that has been in place since the 1992 Council Decision. ‘Network and information security’ policies would after more than two decades be addressed in binding legislation at the EU, rather than national level.

The proposed Directive contains legislative obligations for Member States to adopt national strategies and action plans and to set up CERTs (Chapter II, articles 4-7), as well as cooperate with one another by sharing risk and incident information and installing early warning systems, coordinated by ENISA (Chapter III, articles 8-13). In addition, the proposal imposes minimum security requirements, security breach notifications and enforcement on ‘market operators’ (Chapter IV, articles 14-16). These obligations are without prejudice to those arising from the data protection regime (article 1[5]). Determining the details of a range of these provisions is often delegated to implementing acts adopted by the Commission. The Commission grants itself substantial authority: implementing acts have binding force unless Council or Parliament opposes (article 18[2-5]).

Definition

The definition in article 3[2] of the Directive is nearly identical to the definition formulated the ENISA Regulation 2013 mentioned before (section 2.1):

"security" means the ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system;

---

183 According to recital 25, the concept of security by design is clearly excluded from the regulatory measures in article 14.
The recitals, explanatory memorandum and other accompanying documents do not provide any argumentation as to why the definition is chosen, or what it implies. Neither does the documentation explain why the definition has been slightly adapted compared to the definition of the ENISA Regulation: ‘unlawful’ has been removed from the definition, while ‘events’ and ‘actions’ have been changed into ‘action’.184 In that sense, the Commission still fails to provide guidance how to balance the security attributes of the c.i.a.-triad. But the fact that the c.i.a.-triad, is, as a first, comprehensively adopted in a EU Directive with actual network and information security measures provides an opportunity to develop a vision of what security means, and how its underlying values should be balanced against one another.

Scope

The scope of the proposal is determined by two different definitions, i.e. ‘network and information system’ and ‘market operator’. The ‘market operator’ category contains several exemptions that exclude critical communications providers from the security provisions of the Directive. Taken together, what remains is a regulatory patchwork that both fails to provide legal certainty to providers, and to meaningfully address end-user interests.

Chapter II and Chapter III of the Directive cover ‘network and information system’ policy, and contain regulation on a.o. national strategies, capabilities and international cooperation. The Commission proposal contains a definition for ‘network and information system’ in article 3[1]:

“network and information system” means:

(a) an electronic communications network within the meaning of Directive 2002/21/EC,

and

184 Perhaps ‘unlawful’ was removed to make clear that the Directive would not have any impact on legislative action in the field of cybercrime. The proposal clearly excludes criminal law from its scope in article 1[4].
(b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of computer data, as well as
(c) computer data stored, processed, retrieved or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance.

Again, the proposal and its accompanying documents do not provide any guidance on the definition itself. Sub a directs that the term is broader than networks regulated under the Telecoms Package (see section 2.3). But sub b and c rip the issue open. The concepts of ‘devices’ and ‘computer data’ seek to capture data in electronic form – as opposed to non-electronic data (such as paper file systems). While not motivated by the Commission, the choice to copy the definitions from the 2013 Cybercrime Directive implies that the provisions of Chapter II and Chapter III on national strategies, capabilities and international cooperation cover as broad a ground as ‘cybercrime’ law; all electronic systems and data (see section 2.5).

For Chapter IV, however, the Directive also creates subset of actors under the definition of ‘market operator’. Along with public authorities, the security obligations of Chapter IV of the proposal would only apply to this set of ‘market operators’. The term ‘market operator’ is defined in article 3[8a] and article 3[8b], with a non-exhaustive list in Annex II:

(a) provider of information society services which enable the provision of other information society services, a non exhaustive list of which is set out in Annex II;
(b) operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a non exhaustive list of which is set out in Annex II.

The definition of ‘market operator’ identifies two groups. Firstly, the proposal specifically identifies several critical infrastructure sectors in Annex II (sub b). It bypasses the Council and Member State control of the designation of
European Critical Infrastructures (see section 2.1.). This is probably an unrealistic aim for the final Directive, as the EU Council has already voiced critique.\footnote{In its first debate of the proposal, the Council has already criticized why some sectors had been included and others not, and what the impact of the definition would be on the competitiveness of industry and innovation. 2013/0027(COD), Debate in Council, 6 Jun. 2013.}

The second group covered by the ‘market operator’ definition are the so-called “information society service providers”\footnote{See article 1[2] Notification Directive 1998/48/EC: ‘Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.’} that “enable the provision of other information society services” (sub a – discussed in section 2.3.)\footnote{The element of “enabling” was probably inserted to focus on negative consequences of one service for another service, perhaps in the spirit of critical infrastructures. Recital 24 is quite unclear in its wording, but the term ‘disruption’ in the recital might point at a focus on availability interests, when one service depends on another. The Impact Assessment seems to confirm this reading: “we consider relevant those actors whose services, delivered through the Internet, are empowering key economic and social activities and which have a significant impact in case their activities are suspended for a couple of hours.” SWD/2013/032 final, Impact Assessment, see <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013SC0032:EN:NOT>, accessed 2 September 2015.} Annex II and the Impact Assessment of the proposal point at which providers would fall under the definition: e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services and application stores. According to the Commission, providers that offer similar functions in communications, such as providers of smartphone apps and some VoIP providers,\footnote{See section 1.1.3. for a detailed analysis of VoIP providers under the Telecoms Package.} don’t fall under the definition.\footnote{Impact Assessment - SWD(2013)32 final - 7/2/2013.}

The ‘market operator’ definition and the explanation of the Commission are problematic for several reasons. If one strictly follows the definition of an “information society service”, many apps would also fall under it, rendering the
explanation of the Commission incorrect.\textsuperscript{190} Moreover, from an end user perspective, there is direct interaction with the information society services at the edge of the information value-chain – such as apps. Users directly depend on app security measures and obligations to protect their confidentiality and integrity interests. For a user, there is no difference between accessing Facebook via your browser or via the app and chatting with a friend via the Facebook app or any other instant messaging app. A functional and user-centric approach would apply the security requirements and breach notifications of article 14-16 to all information society services. The proposal seeks to cover user interests with the data protection and Telecoms Package references in article 1[5], but fails to appreciate that these policy cycles leave large gaps in end-user protection. The Commission does not contemplate the full range of the c.i.a.-triad, and how to balance these interests. In this policy cycle, at least, such a comprehensive approach would be consistent with its definition of ‘security’ articulated in article 1[3].

Even within the limited ‘market operator’ definition, a large number of actors are actually exempted from the security measures of article 14. Three exemptions are relevant to communications security. First, according to article 1[3], ‘electronic communications’ and trust service providers are exempted from the relevant security provisions and referred to their respective regulatory regimes in the Telecoms Package (see section 2.3) and encryption regulations (see section 2.4). Especially with regard to the latter, the current regulatory regime does not provide similar security measures, and it remains to be seen whether the 2012 Commission proposal for an eID Regulation will contain such measures after the legislative battle in the Council and Parliament.

\textsuperscript{190} Any app store lists thousands of apps that are a “service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.” The definition is discussed in section 1.1.3.
Second, article 14(8) exempts micro-enterprises with a personnel of 10 or below and an annual turnover or balance sheet of less than 2 million Euro. Recital 27 and the explanatory memorandum provides no additional explanation. The Impact Assessment contains one sentence that again points at prioritizing continuity of service provision for other businesses, rather than confidentiality or integrity interests of end users. Balancing the regulatory burden on start-ups with the persistent problem that security only comes as an afterthought in product and service development is one of the pressing challenges in communications security policymaking, but the Commission does not start with developing a vision how to address it.

Third, and most importantly, soft- and hardware developers do not fall within the scope of the Directive altogether, and are explicitly exempted in recital 24. This goes to the heart of security policymaking, as all information and communications practices depend on soft- and hardware. Their persistent vulnerabilities are a fundamental problem in information and communications security. Even in the survey conducted by the Commission for its Impact Assessment, 36.1% of the most frequent incidents are reportedly caused by soft/hardware failures. The field of security economics illustrates that software vulnerabilities are not so much a technical problem, but are caused by deep market failures in the industry: information asymmetry, liability dumping, ‘winner takes all’ and network externalities all apply. Correcting market

---

192 “On the other hand, micro companies are less critical for the overall continuity of the services given that incidents affecting them may not have a sufficiently wide reaching impact on society as those incidents affecting larger businesses.” SWD/2013/032 final, Impact Assessment, see <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013SC0032:EN:NOT>, accessed 2 September 2015.
194 One of the first papers to address the security economics of software vulnerabilities is Anderson 2001, particularly p. 359. A more recent survey paper is Moore & Anderson 2011. The paper presents an overview the field of internet security economics, and points to dozens of
failures may call for legislative intervention, or in any event its consideration. Exempting these actors from the Directive altogether seems indefensible, but the Commission fails to even attempt to elaborate upon its choice, merely stating that “software developers and hardware manufacturers are not providers of information society services and are therefore excluded”\textsuperscript{195}

\textit{Recent Legislative Action}

The legislative action around the proposed Directive will be the essential indicator of the ambitions of the EU lawmaker in the field of communications security. The proposal has now been under consideration by the Parliament and Council for over two years; both EU institutions seem critical. The Council seems to advocate voluntary approaches for coordination on the EU level and the possibility of (bilateral) legislative action at the Member State level,\textsuperscript{196} the same approach that has been advocated since 1990 (see section 2.1.). The European Parliament amendments of 13 March 2014 already exclude information society services altogether.\textsuperscript{197} At the time of writing, the proposal is still at the EU Council for its first reading, so it is even unclear whether the proposed Directive will ever come to existence at this point.\textsuperscript{198} The Member States are very reluctant to coordinate on the issue, leading to gridlock since the fall of 2014.\textsuperscript{199} But on the face of it, robust conceptualizations of ‘security’ or substantial security measures seem far from being adopted.

\begin{footnotesize}


\end{footnotesize}
2.7. **Historical Analysis of EU Communications Security Law**

It has become a cliché to claim that networked communications challenge existing concepts, and that communications security has become a top policy concern. Much more surprising is the fact that so little research has been conducted on the actual conceptualizations in EU ‘security’ policy. The descriptive, internal legal analysis of the previous sections enables an evaluation of current ‘communications security’ conceptualizations in the EU regulatory framework. What insights has the historical analysis generated about the current state of information and communications ‘security’ legislation, its definitions and its scope?

The historical analysis of the previous section enables the identification of five distinguishable policy cycles in EU network and information security policymaking: data protection, the Telecoms Package, encryption, cybercrime and network and information security. The definitions of ‘security’ in these cycles were mapped and analyzed against the c.i.a.-triad, a consensus conceptualization of ‘security’ in computer science literature. The following figure summarizes the current state of affairs in EU ‘security’ policymaking:

<table>
<thead>
<tr>
<th>E.U. ‘Security’ Conceptualizations</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection</td>
<td>Personal data, may include network</td>
<td>Personal data, may include network</td>
<td>Personal data, may include network</td>
<td>Controllers and Processors</td>
</tr>
<tr>
<td>Telecoms Package</td>
<td>Communications and information**</td>
<td>unclear, probably only personal data</td>
<td>priority issue, but phrased as ‘integrity’</td>
<td>Network and Service Providers in Telco Markets</td>
</tr>
<tr>
<td>Encryption</td>
<td>undefined, linked to data protection</td>
<td>undefined, prioritized in Annexes</td>
<td>undefined, not covered in provisions</td>
<td>Qualified Trust Service Providers</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>undefined, but covered in provisions</td>
<td>undefined, but covered in provisions</td>
<td>undefined, but covered in provisions</td>
<td>Any system, device, all computer data</td>
</tr>
<tr>
<td>Critical infra. and “NIS” proposal</td>
<td>not yet, but explicitly in Directive proposal</td>
<td>not yet, explicitly in Directive proposal, adds ‘authenticity’</td>
<td>not yet, but explicitly in Directive proposal</td>
<td>network and information system, ‘market operators’</td>
</tr>
</tbody>
</table>

* does not cover temporary availability

** ‘information’ in terminal equipment (‘cookie provision’)

---

71
The historical analysis of EU communications security legislation has rendered new insights into its conceptualizations and policies. Five policy cycles have been distinguished in this study: data protection, the Telecoms Package, digital signatures and certificates, cybercrime and network and information security. The historical analysis of these cycles has been synthesized in this chapter, resulting in new research questions that warrant further research to address the central research questions of this study, i.e. how European law should protect communications security.

The historical analysis informs us how ‘security’ definitions are incomplete and left unexplained by the lawmaker. There is no coherent understanding at the EU level about how to define ‘security’, and how its underlying values operate, relate or should be interpreted. Whenever a substantial security breach has occurred, legal protection as well as enforcement structures in data protection and telecommunications – policy cycles that in themselves leave considerable areas of communications confidentiality, integrity and availability untouched – have been re-wired or stretched to address political or economic concerns. Often, this has occurred in ways that are understandable from a practical policymaking perspective, but with conceptually questionable, as well as sub-optimal or outright damaging outcomes in the short and long run.

Between the policy cycles there exist substantial gaps in the application of the c.i.a.-triad in itself, and how its elements should be understood in the various ‘security’ policies adopted in legislation. The obvious connection of the c.i.a.-triad with fundamental rights values – and a long tradition of ECtHR case law – has only been made in the earliest CoE Cybercrime policies, but never since been further elaborated on at the EU level. Furthermore, the institutional ecosystem in the field of network and information security – embodied by ENISA – has quite deliberately not been graced with a competence to work out a coherent vision on communications security policy. Meanwhile, the five
policy cycles have not been ‘scoped’ with communications security in mind, but rather confronted with a myriad of interests, ranging from market structuring in telecommunications, via data protection, to cybercrime and especially national security as powerful policy aims that have overshadowed communications security. The EU regulatory framework contains, in sum, a large amount of legislative arrangements on communications security, but both a coherent vision on part of the lawmaker as well as a clear view of what laws exist and how to apply them is lacking. Legal uncertainty permeates EU communications security law.

A legislative habit seems to exist in which ‘security’ conceptualizations are copied from previous documents, with little argumentation and elaboration on what impact a particular conception of ‘security’ has on the actual policies furthered in these instruments. Regardless of fundamental rights at stake and a robust computer science literature, the critical details are often delegated to the European Commission or standardization processes, rather than negotiated between Council and Parliament. Perhaps conceptual copy-pasting is not that surprising, as loss of institutional memory on a technical and complex policy issue seems an inherent drawback with regard to communications security regulation at the EU level. Nonetheless, the lack of clarity and coherence when it comes to EU security conceptualizations has allowed powerful actors to paint communications security any color they like.

The ‘network and information security’ policy cycle is a case in point (section 2.1 and 2.6). Starting already in 1990, in 2014 EU level network and information security and critical infrastructure policy by and large remains voluntary, and under the control of the Member States in the EU Council. A complex policy surface has emerged: many Member States see communications security as synonymous with national security policies. From the outset, an implicit aim has been to obstruct EU institutions from active
involvement and coordination, as ‘national security’ is explicitly excluded from EU competence under its Treaties. A patchwork of mostly voluntary action plans and public-private partnerships has emerged, while critical actors such as software vendors are exempted from regulatory instruments. In practice, nobody has a clear overview of what policies are in place, who is affected, and across the board, hardly anyone follows ENISA’s voluntary policy advice.

The issue statement of the 1992 Council Decision is worth citing again, both because its aims have clearly not been reached and because it reads like any policy document today:

“1.1. Issue - security of information systems is recognized as a pervasive quality necessary in modern society. Electronic information services need a secure telecommunications infrastructure, secure hard- and software as well as secure usage and management. An overall strategy, considering all aspects of security of information systems, needs to be established, avoiding a fragmented approach. Any strategy for the security of information processed in an electronic form must reflect the wish of any society to operate effectively yet protect itself in a rapidly changing world.”

The policy priority for private communications security has come in bursts. Two timeframes of note are the 1990s – amidst data protection and encryption policy reform (the so-called crypto wars) – as well as 2013 and beyond. Many of the security measures most security experts call for today (end-to-end encryption obligations, private key storage prohibitions obscuring key escrow for CAs), were also proposed back then by the European Commission, only to be removed from EU legislation by the EU Council’s national governments. In the middle of these two timeframes sits a decade of national security and cybercrime securitization practices, intensified by post-9/11, Madrid and London terrorist attack politics.
The year 2013 has seen considerable legislative action in all five policy cycles, which points at the momentum and concerns over communications security at the EU level. Particularly, the ‘Network and Information Security’ Directive presents an opportunity to work out how to conceptualize ‘security’ in EU law and policy. Most if not all of these initiatives will be discussed well into 2015. It is still unclear what coalitions will be formed on this subject after the European Union elections of May 2014. On the one hand, the recent attention for communications security will undoubtedly be exacerbated by the Snowden revelations. On the other hand, the recently proposed Network and Information Security Directive appears to already have been captured by powerful security interests both on the state and corporate side: software vendors are left outside its scope, specific security measures have been weakened by both Parliament and Council and politicians across parties have voiced a desire to delay the legislation for the foreseeable future, hardly responding to widespread concern and media reporting on insecure communications.

The current status quo of conceptual ambiguity is untenable. The importance of, and dependence on, networked communications in economic, social and political life is increasing. At the same time, the weaknesses of these communications are exposed on a daily basis by media reports on poor security practices at service providers or pervasive surveillance practices by nation states all across the world. With regard to the latter, we are only starting to develop a more thorough understanding of the national security dimension in surveillance practices as well as communications security policymaking, enabled through the leaks of Mr. Snowden. Surely, more leaks exposing insecure communications will follow in the coming years. The social dynamics of networked communications, the political situation in the EU and the continuing Snowden revelations create an urgent societal relevance for further research.
2.8. Conclusion

The historical analysis of Part I has provided one of the first comprehensive historical and descriptive overviews on EU communications security law. The study distinguished three phases in EU communications security policymaking. The recent spur of legislative activity, roughly since the start of 2012, across five policy cycles constitutes the third phase. A second phase of relative inactivity stretches roughly from the end of the 1990s until 2012. The first phase starts in 1990. In the early and mid-1990s several bold legal proposals emerged from the European Commission across policy cycles. In 1995, the telecom package saw a strict obligation for providers to encrypt communications end-to-end. In the digital signatures and certificates cycle, the Commission also proposed an explicit prohibition for ‘Trusted Service Providers’ (such as Certificate Authorities) to store the private encryption keys of issued certificates. Around the same time, early E-Commerce Directive proposals mandated Member States to abstain from restrictions on encryption. Interestingly, without any further explanation, not a single one of these proposals ever made it into legislation. The current third phase of EU communications security legislation shows a renewed legal and political momentum for the EU legislature to protect communications security for end users. The adoption of the Lisbon Treaty and the EU Charter of Fundamental Rights, a surge in publicized breaches and the Snowden disclosures may add to the momentum and spur a legal necessity to provide increased protection through EU law based on fundamental rights obligations.

This chapter has revealed the enormous task that lies before the EU lawmaker. Currently, EU law leaves security definitions unexplained in recent instruments and mostly just copies definitions across policy cycles. Some instruments develop confusing definitions of their own, such as the security requirements of the Telecoms Package. The scope of existing legislation is affected by a legacy
of legislating communications security as an afterthought in policy cycles with different aims than addressing communications security in mind. These instruments focus on conventional providers such as Internet access providers or on concepts such as ‘personal data’, rather than protecting communications regardless of technologies or intermediaries that mediate the communication at hand. The security provisions in place are mostly concerned with availability and the continuity of the digital economy; hardly informed by robust insights from fundamental rights or the state of communications security and socio-technical realities at play. The legislature thus fails to provide necessary guidance as to the meaning of ‘security’, its underlying values and how to balance competing interests. Part I concludes that conceptual ambiguity, legal uncertainty, weak enforcement and a patchwork of afforded protection permeate EU communications security law.

A coherent vision on how to legislate communications security across the policy cycles is lacking. This is understandable. Law- and policymakers generally struggle to regulate technologically complex dossiers, such as communications security. At the same time, institutional politics and national security have played a large role in the last three decades. While the EU lawmaker traditionally has no competence in issues of Member State national security, new socio-technical realities challenge such traditional conventions. Since the 1990s, digital technology has become more widespread in society, the threat models and underlying interests more diverse and today’s networked environment more complex. Existing legal concepts and tools seem incapable of protecting end-user communications security. In some policy cycles, industry lobbying has led to surprising outcomes, such as the explicit designation of industry interest groups (such as the CA/Browser Forum), rather than public authorities or other neutral oversight mechanisms, as decisive in determining security requirements of regulated entities in the new eIDAS Regulation. Ongoing debates on the Network and Information Security
Directive repeat historical tendencies, with some EU Member States seeking to establish oversight with military intelligence agencies, rather than independent civilian authorities.

Apart from casual general statements, the EU lawmaker has never connected communications security with a rich body of European fundamental rights case law. But communications confidentiality, integrity and availability are increasingly instrumental for the enjoyment of fundamental rights such as communications secrecy, privacy, communications freedom and the new data protection right enshrined in art. 8 of the EU Charter. Data protection policy has recently become increasingly influential in communications security policy, primarily because several national Data Protection Authorities have prioritized data security. But the EU lawmaker cannot rely on data protection to solve all communications security issues. For instance, data protection law does not consider wider fundamental rights at stake in protecting communications security, nor does data protection law offer a toolkit to address systemic vulnerabilities in communications protocols. In conclusion, the current regulatory approaches to protect end-user communications security through EU law seem untenable going forward.
3. Analytical Framework

The historical analysis of the previous chapter enabled some deeper reflection on the conceptual and theoretical issues in the status quo of EU communications security law. In this short chapter, these uncovered issues are reformulated as research themes that subsequently will become the analytical cornerstone of Part II of this study. The following sections look at the definitions (section 3.1), scope (section 3.2), the strategies of security production (section 3.3) and the tension between national security and EU communications security policymaking (section 3.4).

3.1. Definitions: Conceptual Ambiguity

More a matter of coincidence than of coherent application, the ‘security’ conceptualizations of EU law allude to the consensus definition of the c.i.a.-triad in computer science literature: protecting the confidentiality, integrity and availability of communications to authorized entities. These connections to the c.i.a.-triad are prominent throughout the first influential ‘security’ laws of those early years: the CoE data protection convention, the CoE cybercrime convention, and most explicitly in the 1990 European Commission proposal for a Council Decision ‘In the Field of Information Systems’. EU legislation has not followed the c.i.a.-triad uniformly ever since, save for indirect references in the Data Protection Directive. The Telecoms Package adopts its own vocabulary or refers to the data protection cycle, encryption policies refer to data protection for terminology as well, while recent cybercrime legislation of the EU does not follow the c.i.a.-triad at all. Very recent proposals in the ‘network and information security’ policy cycle refer explicitly to the c.i.a.-triad, once again. But a coherent vision on how to define ‘security’, or a well-informed decision to leave it undefined, is lacking. It seems that copying definitions from earlier documents has become the modus operandi.
In legislation, concepts and definitions are essential. They create the necessary framework for interpreting the intentions of the lawmaker for other regulators, such as supervisory authorities or standardization bodies. Currently, the concepts and definitions are unclear, the details of ‘security’ policies are often delegated to the executive branch of the EU or to standards bodies without normative input. Delegation without guidance make the conceptualization of ‘security’ at the EU level somewhat of an empty vessel. Open norms may be perceived as norms open for debate, rather than general rules to comply with.²⁰⁰

This does not only leave a patchwork of protection across EU communications security law, it also fails to offer guidance as to the meaning or intentions of the lawmaker in a particular instrument, in particular, how to balance underlying interests in delegated acts, implementing laws, or devolved regulatory activity.²⁰¹

In 2005, Nissenbaum observed ‘two quite distinct and incompatible conceptualizations of security’ that ‘vie for public and expert support’: ²⁰² firstly, the ‘technical conception of (computer) security’, rooted in computer science and engineering literature. Secondly, ‘cybersecurity’ emerged as a new concept in policymaking in the late 1990s, tied to a political conception of ‘security’ that has a long history in political discourse and organization.

Systems Design Perspectives

²⁰⁰ Baldwin et al. 2011, p. 67.
With its initial traces in the academic literature in the early 1970s, the technical conception of security – the c.i.a. triad – remains influential in systems design, scholarship, technical standards and, while not coherently, in EU legislation. It spurs the research question if, and how the c.i.a.-triad constitutes a useful conceptual framework for legislating communications security. Since the 1960s, a body of technical literature, primarily in the computer sciences, has been establishing definitions and concepts of technical security. A review of computer science literature will be conducted to provide more clarity into the usefulness of the c.i.a.-triad for legislating communications security. The theoretical foundations of this conception of ‘security’ will be further described and developed in chapter 5.

**Political Perspectives**

The political conception of security is one of the reasons of existence of the nation state. But conceptual ambiguity abounds around understanding what it constitutes, especially in relation to the European Union and networked communications. Nissenbaum argues that ‘cybersecurity’ provides political leverage for including a wide range of interests into cybersecurity policies – beyond the technical conception of ‘security’. These include national security, law enforcement, cyber warfare, critical infrastructure protection and intellectual property protection. With regard to the networked communications environment, focusing on US and NATO policies, Hansen and Nissenbaum argue in 2008 that ‘cyber security has been successfully securitized’. Securitization has fundamental implications for the legislative process, as it comes at the expense of objective facts and evidence.

---

The current legislative and policy dynamics at the EU level beg the question what conception of security the legislature is after: is it protecting the technical conception of security, or might we be witnessing the dynamics of ‘securitization’? The ‘cybersecurity’ narrative can be witnessed at the EU level across the policy cycles. But, contrary to the federal structure of the US, the lack of national security competence of the EU legislature complicates successful securitizations of cyberspace at the ‘federal’ level of the EU Security in its classic, political conception remains a task of the individual Member States; efforts to build European armies and intelligence agencies let alone a coherent foreign policy are in its infancy, and seem only marginally realizable. Against this background, what are the implications of further politicizing technical ‘security’ by the EU lawmaker? The political science of ‘security’ conceptualizations and policymaking at the EU level is a necessary subject of further research to understand the implications of legislating communications security by the EU. It is the subject of chapter 6.

Fundamental Rights Perspectives

In addition to systems design and politics, the security attributes confidentiality-integrity-availability correlate with core fundamental rights ensured in the European Union. These include communications secrecy, privacy, data protection and communications freedom. In addition, communications security has become instrumental in the enjoyment of a broader range of fundamental rights, such as freedom of religion, thought and association. ²⁰⁶ To further study these observations, the study adopts a fundamental rights perspective on communications security in chapter 4.

²⁰⁶ Strandburg 2008.
Feintuck observes that “the establishment of a coherent structure of context-specific substantive values and principles is a necessary prior task to effective regulation in pursuit of public interest objectives.”207 These substantive values are fundamentally derived from the constitutional values of legal systems. Mirroring the core of the cultural, social and economic fabric of a legal system, constitutional concepts come closest to a longer term consensus of what constitutes a just society.208 Feintuck argues that these need to be made explicit to achieve regulatory legitimacy.209 Faced with continuous and accelerating socio-technical change, vulnerabilities and breaches, a firm understanding of the underlying values at stake may be critical to provide the “practical and effective” protection of fundamental rights required by the ECtHR. Additional insight into this question will provide conceptual clarity and may guide the lawmaker in how the security attributes should be translated into security goals and balanced in specific circumstances from a fundamental rights perspective.

Communications confidentiality has been protected under the ECHR since its inception in 1950, and has been recognized as a prima facie constitutional value in European nations for centuries. EU communications security laws hardly elaborate upon this dimension, other than including a somewhat empty reference to fundamental rights in a recital or explanatory document. The E-Privacy Directive is the notable exception to the rule, and its narrow scope has been stretched to include new stakeholder in the E-Privacy debate with the aim of offering much needed protection; a pragmatic approach that cannot be maintained going forward.210 The explanatory memorandum of the Cybercrime

---

207 Feintuck 2010, p. 42.
208 Arnbak & Van Eijk 2012.
209 Feintuck 2010, p. 56.
Convention of the CoE mentions five ECtHR cases that regulate any cybercrime policy.211

Several recent cases of European fundamental rights courts establish positive obligations across Europe to protect communications security through legislation. The landmark April 2014 case delivered by the Court of Justice of the European Union (‘CJEU’) annulling the Data Retention Directive is the latest in the series. It establishes a positive obligation for the EU legislature to ensure communications security as part of its commitment under the EU Treaties. But the development of this doctrine is still in its infancy, which begs the question what fundamental rights obligations the legislature must take into account with regard to protecting specific communications. The Snowden documents have spurred several new court cases to end up before the ECtHR in due course. Meanwhile, the European Union must comply with the ECHR and its case law – European Commissioners for the first time took an oath to uphold the EU Charter of Fundamental Rights in 2010.212

These important legal and political developments exacerbate the harm done by the general lack of normative vision in current EU policies, and add to the relevance of the fundamental rights dimension of the c.i.a.-triad as an important topic for further study. What fundamental rights doctrine can we extrapolate from CJEU Digital Rights Ireland, and expect from the series of ‘Snowden cases’, that current and future EU legislation should take as a general baseline for protecting communications security?


3.2. Scope: ‘Personal Data’ and ‘Actors’

Across EU legislation, a manifold of security prefixes have been observed: data-, information-, network-, communications- and Internet security; to name just a few. Policy legacies underlying the different scoping concepts in EU law have led to a patchwork of protection when it comes to communications security, for instance in its path dependency on the ‘data protection’ policy cycle and ‘actor’-based definitions in the Telecoms package. Could the patchwork be resolved through adopting different conceptual approaches to the protection of technical ‘security’?

‘Actor’-based Scope

In three of the policy cycles – the Telecoms Package, digital signatures and certificates and the ‘network and information security’ – the scope of the leading legislative instrument is determined by whether or not a provider falls within a certain definition of an ‘actor’. Providers offering the same communications functions can be regulated (or not) in completely different ways, because the provider happens to be (or not) a ‘qualified trust service provider’, ‘information society service’, a ‘public electronic communications service’, or the completely ambiguous notion of ‘market operator’ as introduced in the proposed NIS Directive.

The status quo continues to leave gaps in legal protection. In recent years, the networked communications environment has seen rapid change with digitization, convergence and wide user adoption of networked electronic communications in desktop and mobile environments. Threat landscapes are constantly evolving. New companies that provide services that nobody could have imagined yesterday, have already become multi-million enterprises before the EU lawmaker noticed their existence. Basing private communications
security protection on legal instruments that have been adopted with other policy rationales in mind, such as data protection or market structuring reasons (such as the Telecoms Package), puts EU communications security law on a wrong trajectory. The data breach notification in the Telecoms Package adopted in 2009 is a case in point (see section 2.3), as it does not cover a vast range of new communications providers. Even in 2015, these new communications providers still do not have to report data or security breaches.

Actor-based scope definitions are sometimes crafted with different policy rationales in mind, most prominently the harmonization of the internal market of the EU. In the case of VoIP providers, the Telecoms package merely includes new manifestations of networked communications when they operate in similar markets that are regulated to counter the risk of significant market power; so VoIP falls within the Telecoms Package when it competes directly with fixed telephony (in case of SkypeOut, see section 2.3). The vast majority of VoIP communications that do not compete on the market, but offer nearly identical functionality (voice communications) go unregulated. In an internal market mindset that is usual to EU law, market considerations can stretch the scope of the Telecoms Package, but communications security considerations cannot. It points towards the current priorities of the EU lawmaker in this particular instrument. Protecting private communications is not among them.

Numerous examples exist that provoke deeper research in communications security protection in horizontal relationships. Article 5 of the E-Privacy Directive protects the confidentiality of communications. In the Phorm-affair, ISP British Telecom had started pilots in which Phorm, an advertising company, was allowed access to customer communications to deploy deep packet inspection on Internet traffic for commercial, advertising purposes. Upon a lax reaction by the British government, the affair was covered throughout the British mainstream and global tech media, spurring involvement from the
European Commission to sue the UK for failing to implement article 5 E-Privacy Directive. Justifiably so, as BT and Phorm clearly violated the confidentiality of communications under article 5 E-Privacy Directive. Did the affair provoke the Commission to take action because of the harm done to communications confidentiality, or was the fact that there happened to be a law in place, narrowly limited to conventional telecoms companies such as BT – and the fact that the UK seemed not to have fully implemented a legal instrument of the EU – the decisive factor to protect users? To what extent does the Phorm-affair differ substantially from many standard practices employed by ‘information society services’ such as remote computing offered by ‘cloud’ providers today? In terms of private communications security, ‘cloud’ providers employ similar technologies as Phorm by scanning communications by default (such as Gmail), but face much lower legal requirements for communications confidentiality. As such, conceptualizations based on ‘actors’ ignore new socio-technical realities that deeply impact fundamental rights.

In another example, how should EU communications security law respond to recent STARTTLS downgrade attacks by both conventional ISPs and ‘information society services’? Very recently, Verizon and other providers had been caught stripping encryption from e-mail by downgrading the communications protocol STARTTLS to plaintext, in order to allow tracking of users and blocking competitive VPN technologies offered by other service providers. Due to an authentication step preceding the encryption deployment, in which the e-mail servers of sender and recipient signal whether STARTTLS is offered, removing STARTTLS from e-mail impact both ends of the communications. STARTTLS downgrade attacks by e-mail providers,

---
214 See for example Hildebrandt 2013.
regardless of their legal status under EU law, thus not only harmed its customers’ communications security, but anyone e-mailing with a Verizon customer across the globe.

While the European Commission seems to have signaled that the current scope of ‘security’ regulation is too limited, its newly proposed Network and Information Security Directive appears to have the same weaknesses. As noted in section 2.1 and 2.6, its definition of ‘network and information system’ seems broadly defined, but the proposal leans heavily on a new definition of ‘market operator’ that exempts a wide range of critical stakeholders. The actor-approach is, indeed, vulnerable to industry lobbying. The strength of the software and ‘cloud’ lobby in Brussels and Strasbourg is well-known and over decades old. Whether one particular set of actors is covered under the NIS Directive or not is still to be decided by the EU legislature. But, fundamentally, ‘actor’-based scoping is an unsustainable path for the EU lawmaker in its communications security law- and policymaking.

Personal Data Path Dependency

The data protection policy cycle is highly influential across the other policy cycles: article 17 of the Data Protection Directive is often referred without further consideration, and thus determines how ‘security’ is understood and protected in digital signatures and certificate policy as well as for a substantial part of the Telecoms Package. The recently proposed ‘Network and Information Security’ Directive creates another cross-reference in EU ‘security’ policymaking to data protection. In other words, in many of the policy cycles

216 The Business Software Alliance has been critical of the proposed Directive. Now that ‘information society services’ have been excluded from its scope by the EU Parliament, BSA members are no longer regulated under the proposal. Now, the BSA welcomes the legislation on its website: ‘BSA Welcomes European Parliament Vote on Proposed Network and Information Security Directive’, Strasbourg 13 March 2014, see <http://www.bsa.org/news-and-events/news/2014/june/eu06062014eusecurityrules>, accessed 2 September 2015.
communications security protection and enforcement will depend largely on how ‘security’ is conceptualized in light of the ‘personal data’ conceptualization, and enforced in its policy cycle. Conversely, any change in data protection policy has immense impact on other policy cycles, even though ‘security’ concerns were thought to be covered with a simple reference to article 17 Data Protection Directive.

The near future sees the adoption of a new regulatory framework for data protection. The debate on the viability, usefulness and normative force of data protection is probably as current as ever. While this study will fully discuss the proposed update to EU data protection policy in itself, the policy cycle has a large influence on the concept of security and its protection. A crucial development is that the Compromise position of the leading European Parliament Committee LIBE contains the introduction of a ‘pseudonymous data’ category, defined in article 4[2a] of the Compromise proposal for the GDPR: “pseudonymous data means personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution”. A large body of research in computer science has meanwhile established that ‘pseudonymous data’ and ‘anonymized data’ can be re-identified using innovative inference techniques, recently even through writing style. In March 2014, European Commissioner Reding has warned that the pseudonymous data category may become the “Trojan horse at the heart of the Regulation, allowing the non-application of its provisions.” If adopted, data considered pseudonymous data would not be regulated by article 17 (article 30 in the Compromise proposal for the

GDPR), which would imply further limits on the scope of the information and communication security provision through the EU data protection regime.

The data protection lawmaker may not be aware of the impact of its policies in the other policy cycles. In the digital signatures and certificates policy cycle, for example, the silent disappearance of the private key storage prohibition for CAs, a critical security requirement in the 1997 Commission proposal that in the end did not make the 1999 eSignatures Directive, is a case in point. If private keys are stored at CAs, this constitutes a serious security vulnerability once CAs are breached. Information and communications that had been encrypted face decryption if the private keys are obtained. This had been the major concern of security researchers with key escrow, during the crypto wars, as described in section 2.4.

The ‘personal data’ path-dependency may have made the relevance of the omission less obvious. Private keys contain personal data. Understood as a data protection issue, private key storage has become ‘lawful’ by removing its prohibition from the signatures legislation; as such it is merely an issue of ‘consent’ or ‘legal obligation’ as a legal ground for data processing that can be dealt with in a CA’s terms & conditions. But as a communications security issue, private key storage is the ultimate backdoor, a red flag, a glaring vulnerability. In the current legislative debates around its successor, the eID Regulation, the privacy and communications freedom interests are again framed in terms of data protection; the c.i.a.-triad itself is not part of the policy debate. As such, the data protection path dependency has a perverse effect on communications security that is currently not at all understood or even addressed in research and policy.

220 The information security provision itself in the proposed article 30 appears to emerges materially strengthened, with a mandatory data protection impact assessment and security policy requirements.
In its defense, data protection has been stretched considerably in recent years to include communications security vulnerabilities when seen instrumental to protect certain types of personal data. The HTTPS enforcement actions by Data Protection Authorities mentioned in section 2.2 come to mind. Here, the pragmatic approach was informed by public interest, in which data protection indirectly solves a particular communications security issue. Such communications security policy by proxy only occurs because the more appropriate policy cycle has a weak enforcement structure. Data protection may have come to save the day in this example, but gaps in legal protection remain more generally.

Current EU security conceptualizations fail to capture similar communications functions (voice, chat, text, etc.), offered by different providers. The quite imminent pressure on the conventional data protection path dependency and actor-based scope approaches render the following research questions: should a re-conceptualization be informed by the flexible, functional approach taken in fundamental rights law? Could the conceptual scoping weaknesses of the current five policy cycles be avoided? What would a functional approach towards scope look like in EU law? An integral instrument, similar to the data protection regime, existing next to it? Could it provide a holistic approach to communications security policy – both in definition (possibly along the c.i.a.-triad) and in scope? Is it feasible? These questions are addressed throughout the study, particularly in chapter 10.
3.3. Security Strategies: Deterrence vis-à-vis Protection

Communications networks such as the Internet and GSM are, in and by themselves, insecure. Communications security protection has not been baked into their design. Therefore, additional security provisioning is essential to ensure private communications. Several strategies can be seen throughout EU law. As observed in section 2.5, deterrence is a central element in the definition and conceptualizations in cybercrime – and in cyber warfare for that matter. For over two decades deterrence has been the doctrine to drive much of the policy action in the cybercrime policy cycle. Deterrence was the central rationale behind the influential CoE Cybercrime Convention of 2001. Cybercrime policy as a communications security measure can thus be understood as a preventative measure by leveraging a threat of punishment through criminal law – or the law of armed conflict – after the occurrence of an attack.

Deterrence policymaking concentrates on sending credible signals to adversaries to refrain from an attack, because your possible retaliation will cause considerable or devastating harm. But conventional deterrence models are only marginally effective in the field of communications security. It is often impossible to attribute a specific attack to a certain actor (‘the attribution problem’). Moreover, punishing crimes locally is impractical in a global environment. Several crucial nations – including Russia and China – will not join the Cybercrime Convention or any other global cybercrime policy regime.

---

221 See sections 2.3 and 3.4.
222 Preneel & Gürses 2015, p. 2.
223 Citing from a 2010 NATO report of a Group of Experts, chaired by M. Albright, former US Secretary of State: “cyber attacks […] could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under Article 5.” NATO Public Diplomacy Division, NATO 2020: assured security; dynamic engagement, 0753-10, p. 45 & p. 17.
anytime soon. And perhaps most obvious and important, systems actually don’t become more secure by talking tough on punishment and retaliation.\textsuperscript{224}

The Cybercrime Convention recognized already in 2001 that deterrence is a limited doctrine for cybersecurity. The Convention stated in its explanatory memorandum that actual protective measures are “the most effective means” to prevent security breaches, rather than criminal law.\textsuperscript{225} Back then, a broad consensus could be reached with over 50 countries around the Cybercrime Convention and within the EU around the approximation of criminal law, but broad user protection offered through communications security legislation still has to materialize. Meanwhile, the proposed Network and Information Security Directive is struggling for meaningful survival. The deterrence doctrine seems to dominate policy agendas, even though it falls short of providing protection in itself. To further examine the deeper causes of prevailing doctrines, insights from political science need to be studied. Protection as a strategy for communications has many faces and will be discussed in the fundamental rights, systems design and political chapters of this study.

3.4. The EU, Communications Security and National Security

In the start of the 1990s, and across most of the policy cycles, the European Commission suggested c.i.a.-triad inspired communications security conceptualizations and robust policies. The EU Council, however, has been consistently evoking national security as an obstacle to EU competence in the ‘network and information security’ policy cycle. The Council Decision of 1992 was a critical moment in that regard, leaving the main competence in the area of information and network security to European Member States ever since.

\textsuperscript{225} CoE Cybercrime Convention, para. 45.
Since its inception, ‘critical infrastructure’ policy has been framed as a national security issue. Other communications security policy cycles have been substantially weakened. Examples include removing end-to-end encryption as a security requirement in the predecessor of the E-Privacy Directive in the mid-1990s and removing a prohibition for CAs to store private keys of TLS/SSL-certificate customers in the final version of the 1999 eSignatures Directive. The deliberate weakening of encryption standards in GSM in the 1990s that impacted mobile communications security ever since is another case in point.

Thus, we can observe a multi-layered national security capture throughout the history of EU policymaking: i) explicitly in EU Council deliberations and statements by government representatives, for instance when claiming exclusive competence for Member States to legislate technical security or rushing legislative programs through EU institutions, such as the EU Data Retention Directive; ii) implicitly in EU Council amendments to Commission and Parliament proposals for legislation that omit critical provisions, although establishing an empirical connection between national security secrecy can be complicated by the third modality, which is iii) covertly in policy and technical standardization. The latter was illustrated by the GSM case, along with disclosed operations such as the NSA BULLRUN and GCHQ Edgehill programs. Uniquely, the latter class can empirically be attributed to national security capture through the Edward Snowden disclosures.

The historical analysis generates research questions about the relationship between national security capture and regulatory competence at the EU level. On the one hand, history instructs that national governments joined in the EU Council capture most robust policies about to be adopted at the EU level policies by referring to national security, or to surveillance more generally. National security falls under the exclusive competence of national governments – or ‘sole responsibility’ as the EU Treaties have it. This could be seen as a
fundamental weakness in the EU institutional structure to meaningfully regulate private communications security.

On the other hand, the technical and social dimensions of communications security are changing rapidly, and policymaking increasingly affects issues far beyond national security. Rationales for regulatory intervention that come to mind are enhancing the digital economy, harmonizing the internal market, consumer protection and fundamental rights. These are all issues that fall well within EU competence. Considering the increasing weight of other interests involved, not having competence in national security may prove to be an opportunity to actually strengthen security when policymaking concentrates on meaningfully augmenting communications security and harmonizing the EU internal market to that end. In comparison, on the US federal regulatory level, national security is an inherent part of all steps in the legislative process, exacerbated by a near exclusive regulatory authority within the Executive branch based on article II of the US Constitution.226

History certainly suggests national security strategies will remain a potent factor in this debate, for instance as witnessed in the GSM standardization process, and that a national security agenda weakens incentives for meaningfully strengthening communications security on the EU level. Many countries may strategize towards more robust ‘national cybersecurity’ at home, while seeking to foster their ability to engage in intelligence gathering and cyber-attacks abroad. EU level action may impair that ability. Another perspective comes from game theory, highly influential in nation state strategic planning, especially with regard to timing offensive cyber-attacks. Game theory suggests several counter-intuitive incentives with regard

226 See Arnbak & Goldberg 2015.
communications security: securing communications, the theory holds, leads to an escalation of nation state cyber-attacks.\textsuperscript{227}

Recent months have seen considerable legislative action on all five EU policy cycles. Since the 1990s, dependence on communications security in its technical conception has significantly increased on a social, economic and political level. And the post 9/11 obsession with national security appears to be fading to some extent in Europe, at least in the public debate, with the Snowden revelations adding a different policy dynamic to the fold. In other words, the political landscape may change in favor of securing communications for all end-users, rather than keeping communications vulnerable for all attackers.

Such predictions or speculations notwithstanding, the coming years will prove insightful in understanding the competence, political leeway and the ambition of the EU vis-à-vis national security. History instructs that whether or not the EU lawmaker will protect communications security, depends to a large degree on how the issue is framed in the political arena. To understand the legal governance of communications security, and reflect its normative aspects, examining its political dimension – especially vis-à-vis national security – may point towards one of its most impactful aspects.

\textbf{3.5. Summary}

In summary, the historical analysis warrants deeper conceptual analysis to develop more robust foundations for E.U. communications security law. This

\textsuperscript{227} R. Axelrod & R. Illiev, \textit{Timing of cyber conflict}, PNAS, vol. 111, no. 4, Jan. 28, 2014. Weak defences decrease the probability that capabilities for exploiting zero-day vulnerabilities will be deployed, the paper concludes. Increasing overall cybersecurity will lead nation state attackers to rationally strategize towards immediately exploiting zero-days rather than holding on to them in the possible event that ‘business as usual’ escalates into to actual military action.
chapter developed an analytical framework for such conceptual analysis, along the lines of four research themes:

- Security: conceptual ambiguity;
- Scope: ‘personal data’ and ‘actors’;
- National security and E.U. communications security law;
- Security strategies: protection vis-à-vis deterrence.

These research themes form the analytical framework for Part II of the study and are further explored in the following chapters. Fundamental rights analysis of private communications security is the subject of chapter 4. Technical perspectives are offered in chapter 5 and political science perspectives in chapter 6. Part II develops a conceptualization of ‘security’ that will form the basis of the case studies in Part III of the thesis: on HTTPS governance and Snowden’s disclosures around the NSA/GCHQ MUSCULAR operation that intercepted unprotected ‘cloud’ communications on a massive scale. These insights are then integrated in Part IV, that answers the main research questions of this study.
PART II: THEORY AND TOOLS FOR THE EU LAWMAKER

4. Fundamental Rights Perspectives

Philosopher Cicero was among the first to define and defend the confidentiality of correspondence. Over the last centuries, most European nation states independently codified the confidentiality of communications in their constitutions. In over 60 years, the European Court of Human Rights (‘ECtHR’) has developed a rich case law to safeguard fundamental rights protection in electronic communications and respond to challenges emerging from new socio-technical realities. With the adoption of the Lisbon Treaty in 2009, the EU obtained its own constitutional order with the Charter of Fundamental Rights of the European Union (EU Charter). It follows the wording of the ECHR in an article 7 on privacy – although it changes ‘correspondence’ into ‘communications’ – and introduced a separate fundamental right to data protection in a new article 8.

Beyond European fundamental rights law, a September 2014 U.N. Special Rapporteur reiterated a 1988 General Comment of the CCPR on the UN International Covenant on Civil and Political Rights (‘ICCPR’) which held that compliance with its article 17 containing similar wording to article 8 ECHR “requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto”. This chapter seeks to describe and further develop these fundamental rights perspectives on communications security, focusing on the ECHR and EU Charter.

229 Among the first was France in its Constitution of 1791 (3 September, 1791), chapter V, par. 17. See Steenbruggen 2009, p. 40-49.
230 CCPR article 17, General Comment 16/32, §8. In depth in Nowak 1998. On p. 401, Nowak notes this protection of the secrecy of correspondence and telecommunications under article 17 ICCPR extends to cases in which information dissemination systems are operated by private firms.
231 A/69/397, para. 58.
Relatively recently, positive obligations to secure communications security through legislation are starting to emerge from case law of the ECtHR and the Court of Justice of the European Union (‘CJEU’). In addition to existing fundamental rights obligations that follow from the handful of final judgments available, this chapter will scrutinize well-established concepts and tools of European fundamental rights law and where appropriate contextualize these through the lens of several court cases that have been initiated in the wake of the Snowden revelations. These cases, at the apex of national security and communications security, will undoubtedly further pronounce and develop the fundamental rights perspective on legislating communications security. On the one hand, the EU Charter mandates meaningful fundamental rights protection. On the other, EU treaties provide that national security “remains the sole responsibility of each Member State”. 232

Section 4.1 briefly summarizes central concepts of European fundamental rights law. Section 4.2 outlines two recent cases at the ECtHR and CJEU that established positive obligations to legislate communications security. Sections 4.3 and 4.4 then analyze two critical concepts in fundamental rights law: the living instrument doctrine and communications security seen as an ‘objectified first line of defense’. Section 4.5 analyses a critical function of fundamental rights law, protecting users against arbitrary national security interferences. Then, the study argues that the EU lawmaker has a ‘system responsibility’ to ensure the enjoyment of fundamental rights by protecting private communications security through EU law.

This chapter will not bear the character of a textbook on general article 8 ECHR jurisprudence or definitions of privacy. Rather, it specifically focuses on the obligations and options that can be distilled from a fundamental rights perspective on legislating communications security and recent developments in European fundamental rights doctrine. The Snowden revelations have, and continue to shed light on the new threat models that basic fundamental rights are confronted with. These new threat models – that include pervasive passive communications surveillance and active hacking of communications networks on an unprecedented scale – are a cause for a re-evaluation and re-articulation of the fundamental rights perspectives on private communications. As an issue considerably ‘on the move’, developing the fundamental angle on private communications becomes both a necessary and challenging task.

**4.1. European Fundamental Rights Law and Positive Rights**

The central concepts of European fundamental rights law are discussed first, through the lens of the Council of Europe and the European Union. Then, this section describes what positive rights obligations are, how they operate vis-à-vis EU legislation and how they relate to the more classic ‘negative’ rights that limit state power in relation to citizens.

*Council of Europe*

Article 8 of the ECHR contains the right to respect for private and family life, one’s home and correspondence: 234

---

233 Many excellent scholarship already exists that covers these areas. Steenbruggen 2009 presents a thorough overview of communications confidentiality and privacy case law and doctrine until late 2008. Zuiderveen Borgesius 2014 extends the overview, as does this section.

234 In the following, “privacy” and “private life” are used interchangeably. On the differences, see González Fuster 2014.
Article 8, right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 paragraph 1 prohibits interferences with the right to privacy. Paragraph 2 shows that this prohibition isn’t absolute. The right to privacy can be limited in the view of other interests, such as the prevention of crime, or the interests of national security.

The ECtHR interprets the right to privacy from the ECHR generously, and refuses to define the scope of the right. This “living instrument” doctrine allows the Court to apply the right to privacy in unforeseen situations and to new developments. In the words of the Court, the Convention is “a living instrument which [...] must be interpreted in the light of present-day conditions.” The ECtHR subsumes data protection under article 8 ECHR. Moreover, the ECtHR consequently holds that the protection of article 8 ECHR must be “practical and effective, not theoretical and illusory.” As such, the ECtHR sees no obstacle in extending the right to privacy and its “respect for correspondence” to new technologies such as networked communications through the Internet. Steenbruggen has observed that the ECtHR interprets article 8 ECHR more dynamically than any other right in the Convention.

---

235 ECtHR Tyrer v. United Kingdom 1978, par. 31. See also Mowbray 2005 and Steenbruggen 2009.
236 See a.o. ECtHR I. v. Finland 2008; ECtHR S. and Marper v. The United Kingdom 2008, para. 103.
237 ECtHR Christine Goodwin v. United Kingdom 2002, para. 74.
239 Steenbruggen 2009, p. 81.
thus recognizes the contention between new communications technologies and freedom. Section 4.3 further develops these notions.

The ECtHR says the mere threat of a privacy infringement can violate the fundamental right. In a 1978 case regarding a German law that empowered the authorities to inspect mail and to listen to telephone conversations, the Court warned that the “menace of surveillance can be claimed in itself to restrict free communication.” In 1984, the ECtHR said that monitoring communications metadata also interferes with the right to privacy. In the 2008 Liberty case, concerning mass surveillance of telephone calls between the British Isles by government, the Court said that such a “threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants’ [privacy] rights under article 8, irrespective of any measures actually taken against them.” No actual harm needs to be proven for a case to be considered by the ECtHR, nor for the enjoyment of fundamental rights protection under the ECHR.

The ECtHR is the final arbiter concerning concrete cases in which an applicant claims a violation of his or her fundamental rights under the ECHR. As such, it is not to be compared with conventional constitutional courts, to which cases can be brought to challenge the constitutionality of national legislation law itself. Claims ‘in abstracto’, such as a Belgian NGO that filed suit against

240 ECtHR Klass and others v. Germany 1978, para. 37.
242 ECtHR Liberty and others v. United Kingdom 2008, para. 56. See also para. 104-105.
243 This is contrary to US constitutional law, where actual harm needs to be proven in order for a case to be heard. See for instance 68 US, Clapper v. Amnesty International USA (2013), 26 Feb. 2013, in which the US Supreme Court dismissed standing on part of applicants Amnesty International US, the ACLU a.o. as they failed in proving that they had been a subject of alleged surveillance. The statutes that regulate such surveillance effectively deny the applicants to challenge it. See Van Hoboken, Arnbak & Van Eijk 2012.
Belgium for lacking regulation on the deployment of CCTV cameras, fail. At the same time, a victim of CCTV surveillance could challenge the lack of such legislation as a failure of the positive obligation from the state to legislate CCTV according to the strict rules on limiting fundamental rights under article 8(2) ECHR and its case law. When the ECtHR finds concrete violations, a judgment is delivered declaring a state in violation of the ECHR.

European Union

The Court of Justice of the European Union (‘CJEU’) is an entirely different entity than the ECtHR in Strasbourg. One of the main functions of the CJEU is interpreting laws, such as directives, adopted by the European Union. Contrary to the ECtHR, the CJEU can assess national legislation ‘in abstracto’ and find a failure to fulfil obligations under the Treaties and require Member States to take necessary measures to comply with its judgment. The European Commission is then tasked to enforce these decisions. In the case of legislation of the EU, it can “declare the act void” as happened with the Data Retention Directive in CJEU Digital Rights Ireland, discussed in the next section. Upon such a ruling, the act has “never existed”. As the CJEU declared the entire Directive void solely based on the fundamental rights enshrined in the relatively young EU Charter, there had been some confusion about the legal effect of the judgment even within the EU Commission. Among scholars, views range from a foundation of “constitutional

246 Article 260 TFEU.
247 Article 264 TFEU.
248 Rauhofer & Mac Sithigh 2014.
patriotism”, 250 “seeming disinterest in other fundamental rights” 251 to questioning whether the CJEU is finally “evolving from the engine of integration into a proper constitutional court.” 252

The Charter of Fundamental Rights of the European Union (‘EU Charter’) is a document listing the fundamental rights and freedoms recognized by the European Union. The EU Charter was adopted in 2000, and was made a legally binding instrument by the Lisbon Treaty of 2009. 253 The EU Charter copies the right to private life almost verbatim from the ECHR. The CJEU has ruled that the right to privacy in the Charter and the Convention must be interpreted identically. 254 It follows from the EU Charter that its article 7 offers at least the same protection as article 8 of the ECHR. But the EU Charter uses the more modern and technology neutral term “communications” instead of “correspondence” to account for future technological developments. 255

The EU Charter has a separate provision that lists the limitations that may be imposed on the Charter’s rights and freedoms in article 52. Regarding the right to private life, the limitations from article 52 of the Charter roughly correspond to those listed in the second paragraph of article 8 ECHR. 256

---

252 Granger & Irion 2014.
253 See article 6.1 of the Treaty on European Union (consolidated version 2012). The institutions of the EU must comply with the Charter. The Member States are also bound to comply with the Charter, when implementing EU law (article 51 of the Charter).
254 CJEU C-400/10 (J. McB. v L. E) 2010, para. 53. Earlier, the CJEU had already established that a mere threat was already sufficient to rule a violation of the right to privacy, for example CJEU C-139/01 (Österreichischer Rundfunk) 2003, para. 75
255 Toelichtingen bij het Handvest van de Grondrechten (2007/C 303/02), PubEU 14.12.2007, C 303/17
256 See article 52(3) of the Charter Of Fundamental Rights of the European Union; Note from the Praesidium, comments on article 7 (Praesidium 2000).
The EU Charter contains a new set of explicit fundamental rights, notably the right to data protection. Article 8 EU Charter reads:

*Protection of personal data*

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

In recent years, the CJEU has been taking up its role in fundamental rights matters more prominently, whereas until 2009 it had merely directed national legislatures and judiciaries to ensure balanced fundamental rights protection. But the CJEU is still in its earliest stages of formulating the exact meaning and scope of these newly established rights in specific cases, particularly in relation to the long and rich tradition of the afforded protection through the ECHR – to which all EU Members States have signed up and the EU may become a full member in the near future. With regard to communications security, the April 2014 judgment that annulled that Data Retention Directive is the very first occasion the CJEU could rule on the matter.

*Positive Obligations*

---

257 Another ‘new’ fundamental right is the freedom to conduct a business of article 15 E.U. Charter. As the right has not yet been mentioned in the context of communications security case law, this study does not comprehensively discuss ‘the freedom to conduct a business’. The right is, however, mentioned in the discussion of CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, as the ruling held that ‘economic considerations’ are an insufficient safeguard to protect the security of the blanket retention of communications metadata as regulated under the Data Retention Directive. See section 4.2.

258 See for example CJEU C-275/06 (Promusicae) 2008.

259 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014.
Positive obligations broadly take two shapes in European fundamental rights doctrine. First, ensuring the exercise of fundamental rights in so-called ‘vertical’ (State-citizen) relationships and second, the more specific obligation for states to introduce specific legal provisions to regulate citizens that ignore or violate fundamental rights – in ‘horizontal’ relationships. Beyond state conduct, states are accountable for a system of laws to ensure fundamental rights protection. In addition, such laws need to be enforced to guarantee effective enjoyment: “regulations to protect guaranteed rights serve little purpose if they are not duly enforced.”

Enforcement comes along with positive obligations.

The ECtHR is the final arbiter on establishing the existence of positive human rights. Over the decades, the ECtHR has developed a ‘fair balance’ test with regard to the existence of positive obligations in the ECHR. In this test, the rights of individuals are balanced against the public interest; Member States have a certain ‘margin of appreciation’ to determine how to balance and protect the rights of the ECHR. Roughly, five criteria will play a role: i) the essence of a fundamental right is impaired; ii) the complexity of the topic at hand; iii) the existence of a European consensus on positive obligations; iv) whether a collision with other fundamental rights is at stake, and v) the vulnerability of citizens.

How to exactly balance the criteria of the ‘fair balance’ test is an unsettled debate in the literature. Since the ECtHR has not developed rigid doctrine on positive rights, and often will tailor these criteria to the issues arising in a concrete case, some have argued that the existence of positive rights is of a somewhat casuistic nature, lamenting a consequent lack of legal certainty. But the ECtHR can only rule on cases before it, and will establish these rights

260 ECtHR Moreno Gomez v. Spain 2004, para. 61
whenever it has a chance to do so. Therefore, as De Hert argues, it is not possible to precisely index positive obligations: “a legal system cannot guarantee that no human rights violations occur, but efforts need to be taken to prevent them and when they occur the system needs to be responsive.”\textsuperscript{263} With regard to communications security, both the ECtHR and CJEU have taken initial steps to recognize its instrumentality for the enjoyment of fundamental rights more broadly - as will become clear in the next section.

With the relatively recent introduction of the EU Charter, the CJEU may seize the moment and bring fundamental rights more to the core of the European project, apart from establishing an internal market.\textsuperscript{264} Recent cases certainly seem to indicate a willingness to do so, especially in cases concerning privacy.\textsuperscript{265} Difficult questions emerge on the weight given to fundamental rights vis-à-vis market integration, the interaction between fundamental rights recognized under the ECHR and ‘new’ separate rights such as data protection and how to deal with the vexing competence issues around EU rulemaking and national security. These questions are addressed in the following sections.

\textbf{4.2. Positive Obligations to Protect Communications Security}

Positive obligations abound with regard to electronic communications and fundamental rights, but the emergence of positive obligations to technical security is a very recent affair – particular measured in ‘constitutional time’.\textsuperscript{266} It is, however, telling that when European fundamental rights courts were provided with an opportunity to reflect on securing information and communications, the ECtHR and CJEU recognized a need to do so.

\textsuperscript{263} De Hert 2012, p. 95.
\textsuperscript{265} Granger & Irion 2014.
\textsuperscript{266} Among the first authors to recognize its existence is De Hert 2012, p. 193-232.
This section develops the positive obligations to protect communications security by discussing in depth two rulings relevant to this relatively new doctrine. In 2008, the ECtHR construed a positive right pursuant to article 8 ECHR in a case concerning health data (‘ECtHR I. v. Finland’). The April 2014 CJEU ruling that annulled the Data Retention Directive (‘CJEU Digital Rights Ireland a.o.’), connects the positive obligations to secure so-called communications metadata to the new fundamental right to data protection of article 8 EU Charter. From these cases, extensively discussed below, fairly specific criteria and clear instructions can be extrapolated that the EU lawmaker must observe when legislating communications security.

**ECtHR I. v. Finland**

*ECtHR I. v. Finland*\(^{267}\) concerns the protection of health data of applicant I., a nurse who worked in a public hospital in Finland between 1989 and 1994. She had been diagnosed with HIV in 1987 and had therefore visited the ‘contagious diseases’ department in the same hospital. She suspected her colleagues knew about her disease because at the time, all employees of the hospital could access her health data. Upon her request, the access to the database was tightened and she was re-registered under a different name. When her contract was not renewed in 1995, she filed a complaint with the authorities to see who had accessed her medical file, as she suspected her contract as a nurse wasn’t renewed because of her disease. The hospital responded that it could not reconstruct who had accessed her file. Only the relevant department and the last five consultations were logged and, at the time, any staff could have accessed her file. Her complaint was rejected, but access controls and logging were strengthened in the sense that logging now included the person accessing...

\(^{267}\) ECtHR I. v. Finland 2008.
the file. Nonetheless, I.’s civil proceedings all failed because she could not prove that her data was in fact accessed, before even being able to prove that she suffered harm because of it. Finally, in 2003, a complaint against Finland was lodged at the ECtHR claiming a violation of article 8 ECtHR. I. claimed that “the district health authority had failed in its duties to establish a register from which her confidential patient information could not be disclosed.” and, as such, “a breach of the State’s positive obligation to secure respect for her private life by means of a system of data protection rules and safeguards.”

Analysis

About five years later, in 2008, the ECtHR unanimously held a violation of article 8 and established a positive obligation for state legislatures to ensure security of personal data in its technical conception. The ECtHR bases its judgment on at least five arguments. Firstly, data protection is central to the enjoyment of fundamental rights. Secondly, data confidentiality is “a vital principle” crucial to both fundamental rights and “confidence in the medical profession and health services in general”. Thirdly, the aim of relevant domestic law was to secure personal data against unauthorized access and the law in the books would have allowed “to strictly police access to and disclosure of health records”. Strict application of the data protection law would have provided a substantial safeguard, but the Court lamented the lack of practical and effective protection afforded because of failing enforcement mechanisms. Fourthly, the Finnish legal system had shifted the burden of proof on I. to prove colleagues had accessed her data. Fifthly, Finnish law merely provided for compensation of damages, and thus failed to ensure that I. could verify these facts in the first place. For all these reasons, Finland failed in its positive

269 ECtHR I. v. Finland 2008, para. 37.
270 Quotes from ECtHR I. v. Finland 2008, para. 38-40.
obligation to ensure the enjoyment of the respect of I’s private life under article 8 ECHR.

ECtHR I. v. Finland has far-reaching implications beyond this specific case. Most crucially, the positive right to the technical conception of security has been established from the general principles of fundamental rights law to the case, rather than from the case-specific facts.\(^{271}\) Including general principles before ruling on the facts had been a trend in ECtHR case law for some time, with the intent to provide more guidance to CoE Member States on the general principles of European fundamental rights law.\(^{272}\) The ECtHR merely applied general principles already inherent in article 8 ECtHR and its case law; this was just the first time in which it had the opportunity to establish such a positive right. The purported unauthorized wrongdoings had taken place twenty years before the final ruling. In other words, one could argue the positive right always existed. In the wake of the case, many authors therefore conclude that data protection legislation, particularly the EU Data Protection Directive, if correctly implemented and enforced, can be seen as sufficient safeguard under the new positive fundamental right under the ECHR.\(^{273}\)

The Court is quite serious about the newly established fundamental right. In the exact wording of the Court: “what is required in this connection is *practical and effective protection to exclude any possibility* of unauthorized access occurring in the first place. Such protection was not given here.”\(^{274}\) While providing practical and effective protection echoes a vast body of earlier case law, the inclusion of the elements ‘exclude any possibility’ places the fundamental rights test on a high level and shows that the ECtHR is sincere when it comes to the positive obligation to technical security. Risk-

---

\(^{271}\) ECtHR I. v. Finland 2008, para. 35-37.
\(^{274}\) ECtHR I. v. Finland 2008, para. 47.
assessments, for instance, that fail to meet this test can be seen as being in breach of article 8 ECtHR. In a 2013 ruling on the retention of DNA data in the context of criminal investigations, the ECtHR finds no violation of article 8 ECHR in a German domestic law that provides additional technical and organizational measures through legislation to exclude unauthorized access to DNA samples by the independent experts that investigate those data.275

The ECtHR reasons in ways that give several specific elements of the case broader impact as well. In terms of scope, while the case covers medical data, the positive obligation extends to all personal data with an intensified scrutiny for those of a sensitive nature. Also, the Court clearly states that while the case concerns a public hospital, a positive obligation exists “between individuals”276 too. The enforcement failures are explicitly lamented.

On a more conceptual level, ECtHR I. v. Finland does not merely highlight the obvious individual and societal interests in data confidentiality, but in data integrity as well. While not explicitly, the ECtHR connects its conceptualization of technical security to the c.i.a.-triad. The argument of the Finnish government that it was not feasible to mandate that the “authenticity of every request could be controlled in advance, since access to the data was often required immediately and urgently” fails in the Court’s assessment.277 Data integrity is held to be essential for individuals to seek justice, and for information societies to deliver it. The fact that I. held the burden of proof in the civil proceedings in Finland was lamented. The burden of proof is a

275 ECtHR Peruzzo & Martens v. Germany 2013 (inadmissible), para. 21 and especially para. 45: “The identity of the individual from whom the DNA sample has been obtained is not disclosed to the experts charged with drawing up the DNA profile who are furthermore under an obligation to take adequate measure with a view to preventing any unauthorized use of cellular material examined. The cellular material itself has to be destroyed without delay once it is no longer needed for the purpose of establishing the DNA profile. Only the DNA profiles extracted from such cellular material may be kept in the Federal Criminal Police Office's data base.”
276 ECtHR I. v. Finland 2008, para. 36.
277 ECtHR I. v. Finland 2008, para. 34.
centerpiece in legal doctrine, and often transferred to users when confronted with breaches of technical security. Here, the Court deems the positive right to technical security – specifically data integrity, by naming access control and keeping log files in this case – as crucial to the enjoyment of the rights ensured under article 8 ECHR. Technical security, in other words, is not only instrumental to privacy but also to the rights to due process and effective remedies in information societies.\footnote{278}

In addition, the loaded concept of security now, at the very least, not only applies to one of the grounds for limiting fundamental rights with regard to national security. Its elevation to fundamental rights status gives technical security a stronger position when confronted with national security. It is central to the enjoyment of fundamental rights afforded by article 8[1], rather than a policy concept vulnerable to the national security capture observed in section 3.4.

\textit{CJEU Digital Rights Ireland a.o}\footnote{279}

As noted, the EU Charter formally entered into force in 2009 with the adoption of the Lisbon Treaty. Before 2009, no positive obligation to protect fundamental rights interests such as privacy or communications confidentiality could be construed from CJEU case law or the treaties.\footnote{280} When confronted with fundamental rights, CJEU case law had developed a tradition of

\footnote{278} Aspects the Court, as ever so often, included in the article 8 ECHR analysis rather than developing them independently under article 6 and 13 that ensure due process and an effective remedy respectively, ECtHR I. v. Finland 2008, para. 50-51. A critical comment is made in Räman 2008, p. 564.

\footnote{279} CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014. Parts of this section will be published in a forthcoming paper, Zuiderveen Borgesius & Ambak 2015.

\footnote{280} Steenbruggen 2009, p. 177. Beyond the adoption of the Lisbon Treaty and the change of attitude in CJEU case law, several authors argue that the E.U. lawmaker already showed a consistent appetite for a positive right to communications privacy since the 1997 when the first version of the current E-Privacy Directive was included the Telecoms Package (see section 2.3). See Steenbruggen 2009 and De Hert 2012.
mandating EU Member States to protect those rights and strike a reasoned balance between them.\textsuperscript{281} A few cases before the CJEU after the adoption of the EU Charter already showed first signs of a change in attitude,\textsuperscript{282} And with \textit{CJEU Digital Rights Ireland a.o} in April 2014, the CJEU firmly annulled the Data Retention Directive and established a positive obligation for the EU legislature to protect the fundamental rights to privacy (article 7 EU Charter) and data protection (article 8 EU Charter), and explicitly mentions the technical conception of security as an integral part of the positive obligation.\textsuperscript{283} First, the origins and history of the Data Retention Directive are outlined. The following discussion of the judgment limits itself to the elements of the ruling relevant for legislating communications security.\textsuperscript{284}

\textit{History}

The Data Retention Directive was adopted in 2006. Since the 1990s, long before 9/11, US and UK authorities have lobbied EU institutions and Member States to adopt data retention legislation,\textsuperscript{285} but it took the tragic London and Madrid events for the UK to arrange a narrow majority support amongst fellow Member States for comprehensive data retention legislation at the EU level. In 2006 it took three months to race the directive through all EU institutions just before the UK presidency of the EU Council ended with the turn of the year; one of the fastest adoptions in the history of EU law making.\textsuperscript{286}

The directive obliged Member States to adopt data retention requirements for telecom providers, such as phone operators and Internet access providers

\textsuperscript{281} CJEU C-92-93/09 (Volker und Markus Schecke GbR v Land Hessen) 2010. Williams 2004.
\textsuperscript{282} CJEU C-70/10 (Scarlet v. Sabam) 2011.
\textsuperscript{283} CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 66-68.
\textsuperscript{284} See for more comprehensive discussion Borgesius & Arnbak 2015; Granger & Irion 2014.
\textsuperscript{286} See extensively Arnbak 2009.
falling within the scope of the Telecoms Package. Examples of data that must be retained are data necessary to trace and identify the source of a communication, such as phone numbers. Other examples are the date and time of the log-in and log-off of an Internet access service, together with the IP address and the user ID of the subscriber or registered user. Member States must ensure that these ‘metadata’ are retained for periods of not less than six months and not more than two years from the date of the communication.

The Data Retention Directive was controversial from the start. The European Data Protection Supervisor called it “the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects.” Prior to the proceedings before the CJEU, high courts of various Member States declared the national implementation act of the directive invalid. Against this background the CJEU had to decide the case on the Data Retention Directive. Furthermore, since 2013 the Snowden revelations have intensified the fundamental objections against unfettered surveillance.

_CJEU Digital Rights Ireland_ concerns questions from referring judges in Ireland and in Austria. The case for the Irish High Court stemmed from a dispute between the organization Digital Rights and the Irish authorities on the legality of national measures implementing the directive. The case before the Austrian Verfassungsgerichtshof entailed constitutional actions brought before that court by the Government of the Province of Carinthia, and by 11,130 other applicants regarding the compatibility of the Federal Constitutional Law with the law implementing the directive.

---

287 Article 3 DRD. See section 2.3.
288 Article 5(1) DRD.
289 See <http://europa.eu/rapid/press-release_EDPS-10-17_en.htm?locale=en>, accessed 2 September 2015. The European Data Protection Supervisor (EDPS) is the supervisory authority responsible for monitoring the processing of personal data by the European Union institutions and bodies (see article 41 of Regulation (EC) 45/2001 on personal data processing by the Community institutions and bodies).
289 See for an overview of the national cases see Kosta 2013.
The referring judges asked the CJEU in 2012 to examine the validity of the Data Retention Directive, in the light of Articles 7, 8 and 11 of the Charter. These rights concern privacy (article 7), data protection (article 8), and freedom of expression (article 11). The CJEU decides that the EU legislature has exceeded the limits imposed by articles 7 and 8 of the Charter and invalidates the directive.

Analysis

In of CJEU Digital Rights Ireland, the CJEU not only firmly establishes a positive right to technical security of communications, but develops the new and concrete elements of the right from both a substantial and procedural perspective. Assuring the security of retained metadata had played a significant role in the build-up to the ruling by the Advocate-General. But the A-G Opinion had advised the CJEU that since most Member States had provided for additional safeguards around access obligations and data security in the implementation of the Directive in national legislation, the Directive should be corrected – not annulled – within a reasonable period. The CJEU would not have it, however. The final ruling leaves no doubt about who was responsible
for the lack of protection afforded: the EU legislature. Moreover, the CJEU has given the EU lawmaker a workable toolkit to protection communications security in current and future EU law.

First the CJEU establishes that mandatory blanket metadata retention amounts to a “particularly serious interference” with the right to privacy enshrined in articles 7 and 8 EU Charter, one that is “likely in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.” Even if that in itself, according to the CJEU, does not in principle “adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8”, it does raise the criteria for safeguards. The particularly serious interference is not balanced by “clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.” Thus, it rules the Directive void in its entirety, the first time the CJEU has ever gone this far purely based on a fundamental rights analysis.

The CJEU explicitly connects its reasoning to ECtHR case law, thus once again declaring that the CJEU follows the general principles of article 8 ECHR directly in a Grand Chamber ruling.

---

295 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 69: “by adopting Directive 2006/24, the E.U. legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter”.
296 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 37.
297 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 40.
298 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 54.
299 The authority to do so is provided by Article 264 TFEU.
300 Such as the general principles outlined in ECtHR Liberty and Others v. the United Kingdom 2008.
In its substantial analysis, the CJEU identifies three areas in which the Data Retention Directive lacks legislation 301 to ensure the “interference being precisely circumscribed by the provisions to ensure that it is actually limited to what is strictly necessary”. 302 This substantive analysis on privacy interferences presents a concrete context for developing data security as the fourth area in which the Directive fails data security. Critically, the CJEU cites the entire body of relevant EU legislation on data security: 303 article 17 of the Data Protection Directive, article 4 and 5 of the E-Privacy Directive, and article 7 Data Retention Directive. The latter reads:

\[
\text{Article 7}
\]
\[
\text{Data protection and data security}
\]
\[
\text{Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:}
\]
\[
(a) \text{ the retained data shall be of the same quality and subject to the same security and protection as those data on the network;}
\]
\[
(b) \text{ the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;}
\]
\[
(c) \text{ the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;}
\]
\[
\text{and}
\]
\[
(d) \text{ the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.}
\]

301 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 56-65; a failure to i) differentiate between data subjects (blanket); ii) regulate lawful access; and iii) specify between these aspects and the retention of specific data categories (unspecified) for certain periods (minimum 6 months, regardless of suspicion or seriousness offence). Therefore, the Directive is not limited to what is strictly necessary.
302 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 65.
303 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 4-16.
In *CJEU Digital Rights Ireland*, the Court rules that the data security regime of the Data Retention Directive fails on two grounds: i) lack of specificity in the law to “ensure full integrity and confidentiality”, and ii) failure of the law to ensure independent supervision.  

The CJEU develops its new doctrine based on the first of these two grounds, which is discussed in detail below.

The first requirement – *specificity in the law to ensure full integrity and confidentiality* – establishes a positive obligation for the EU lawmaker to ensure technical security in the same instrument as the one interfering with it. The CJEU explicitly connects the positive obligation to the technical language of the c.i.a.-triad, whereas the Data Retention Directive, E-Privacy Directive and the Data Protection Directive have not mentioned these exact terms.

Furthermore, the CJEU present a concrete framework for determining to what criteria specificity needs to be adapted “in a clear and strict manner”:

(i) the vast quantity of data (..),  
(ii) the sensitive nature of that data and  
(iii) the risk of unlawful access to that data;  

Then, in a landmark move, the CJEU integrates in its analysis article 4(1) of the E-Privacy Directive and article 17(1) of the Data Protection Directive. It holds that the combination of these laws does not ensure “a particularly high level of protection and security.” In other words, the current legislation based on the standard language of “technical and organizational measures” is insufficient to

---

304 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 66-68. Deeper analysis of the Court’s second requirement falls outside the scope of this chapter, which focuses on the new doctrine the Court develops on the confidentiality and integrity of communications. The Court finds that independent supervision results in an obligation for localizing the storage of retained data on E.U. territory. In the view of the Court, the lack of a legal provision on localization has “the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured.” (para. 68).

305 See sections 3.1 and 3.2.

306 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 66.
protect fundamental rights. The combination of these three Directives, that constitute the very core of the current approach to legislating technical security, in the words of the CJEU:

“permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.”

Economic considerations of market operators alone, the CJEU explicitly rules, does not provide sufficient technical security. The observation works both towards ensuring full integrity and confidentiality and towards commercial motives market operators might have to hold on to these data. Also, the CJEU criticizes the lack of an irreversible data destruction regime to safeguard data protection rights.

Crucially, the CJEU denounces the lack of legislative safeguards in the interaction between the specific Data Retention Directive and general EU laws such as the Data Protection and E-Privacy Directives. Thus, the CJEU questions the entire modus operandi of EU technical security legislation. The hands-off reliance on delegation and self-regulation does not convince the CJEU that “sufficient safeguards, as required by article 8 of the EU Charter, to ensure effective protection against any unlawful access and use of that data” are provided. The CJEU reaches this conclusion notwithstanding the formation of the “Data Retention Experts Group” established by a Commission.

---

307 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 67.
308 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 67. Emphasis added.
309 This study does not comprehensively discuss the new ‘freedom to conduct a business’ of article 15 E.U. Charter, as the CJEU did not consider or even mention the right in its ruling (see para. 23-24). In itself, that fact may indicate that this ‘freedom to conduct a business’ does not come into play when considering technical security safeguards to protect electronic communications.
310 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 67, last sentence.
311 CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 66, emphasis added.
Decision that in a series of guidance documents develops a “closer understanding of the term ‘data security’ in relation to its application in Directive 2006/24/EC.” Indeed, while the Expert Group – comprised of government, industry and law enforcement authorities – comes with several voluntary recommendations to augment security, it established that the Data Retention Directive does not in itself create new security obligations. Contrary to such delegated activity coordinated by the EU Commission, the CJEU establishes that data security must be safeguarded in the same legislation that regulates data use when the aforementioned three criteria are met. The CJEU does not even refer to several data security breaches surrounding retained data that had already been reported in the media across Europe.

Securing communications data is elevated to a central safeguard under article 8 EU Charter – a matter of ex ante legislation to ensure security rather than relying on delegation, economic consideration of market operators, nor ex post incident recovery through other means of law. CJEU Digital Rights Ireland does not stand alone. Earlier decisions illustrate a broader rejection of self-regulation when fundamental rights are at stake.

Coincidentally, scholars of security economics have found similar results in their research since the turn of the millennium. To reiterate: “systems often fail because the organizations that defend them do not bear the full costs of failure.” Here, the CJEU and security economics scholars agree: permitting merely economic considerations will not provide a sufficient level of technical

313 Idem, p. 2.
315 See ECtHR I. v. Finland 2008, para. 37.
316 CJEU C-355/10 (Frontex) 2012.
317 See section 5.5.
security that meets public interest requirements. The important addition of the CJEU is that the public interest objectives originate in fundamental rights.

Secondly, a long discussion has been ongoing on the retention periods of communications data beyond the Data Retention Directive. Particularly, ‘information society services’ have been under scrutiny for their policies regard the storage of sensitive personal data on a scale far beyond metadata alone. Google, for instance, stores vast amounts of personal data on its users far beyond ‘mere’ metadata. Search results, YouTube movies, photos and contact lists are just a few of many sensitive personal data categories. Google’s retention periods seem to be indefinite, or in constant flux at least, an issue that has been flagged by a number of Data Protection Authorities throughout the emergence of these information society services. Since 2012, data across Google’s many services have been integrated into one Google profile per user to enhance its enterprise activities. Apart from exponential increases in marketing inferences that can be made based on the integrated dataset per user, Google now provides a one-stop shop for authorities to request data under lawful access and security legislation not particularly set up with the new realities in mind. Neither legislatures nor supervisory authorities could have foreseen the ways in which today’s information societies have developed. With CJEU Digital Rights Ireland, the Court has unambiguously communicated to the EU legislature that such vast databases cannot exist without “clear and precise” legislation that specifically ensures “full confidentiality and integrity” of the data “against any unlawful access and use of that data.” Quantity, sensitivity and risk of abuse are the central criteria for determining if added

318 See extensively section 2.3. The concept is defined in article 1[2] Notification Directive 1998/48/EC: ‘Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.’
legislation is needed. The new fundamental rights reality since *CJEU Digital Rights Ireland* sets much stricter obligations for EU legislature to ensure data security in contemporary and future information societies.

In sum, technical security seems to be a priority issue in need of proactive protection through legislation that is practical and effective. *ECTHR I. v. Finland* has established the necessity of “practical and effective protection to exclude any possibility of unauthorized access” and elevated the Data Protection Directive to a status of meeting those positive obligations. *CJEU Digital Rights Ireland* requires “rules specifically adapted to ensure full confidentiality and integrity” and “independent oversight”, and presented the EU legislature with a workable framework for assessing when the standard practice of deferring to the Data Protection Directive does not suffice. Communications metadata retention and the Data Retention Directive, controversial from the start, indeed have provided the CJEU with a suitable set of facts to develop its doctrine; failing to do so would have been a missed opportunity. Jointly, the cases have a significant impact on legislating communications security by the EU in the future.

**4.3. A Living Instrument: Scoping ‘Communications’ Functionally**

Part I concluded that current EU legislation provides a patchwork of protection in the realm of communications security. Similar functions in communications such as voice, chat and text are protected depending on which actor is involved in the process, based on regulatory legacies. A data protection rationale is then employed to stretch legislation beyond its formal scope. This section further examines the approaches taken to new technologies by the ECtHR and the CJEU. Consequently, a functional approach to scoping communications security is developed.
The “Living Instrument” Doctrine vis-à-vis Data Protection

As observed in section 4.1, article 8 ECHR adopts not only a broad but flexible conception of privacy. The ECtHR consciously refuses to precisely define the scope of the right to privacy, and rather sees it as constantly evolving. This “living instrument” doctrine ensures that new communications technologies can be included in the scope of protection. The main reason for the living instrument doctrine is that the enjoyment of rights in the ECHR must be “practical and effective, not theoretical and illusory.” The open wording of article 8 and the “living instrument” doctrine of the ECHR are seen as the root cause for the flexibility of the ECtHR and its ability to provide protection regardless of the technological reality of tomorrow. In ECtHR Michaud v. France, the ECtHR once again reiterated this approach in firm wording:

90. In establishing the right of “everyone” to respect for his “correspondence”, Article 8 of the Convention protects the confidentiality of “private communications” (see Frérot v. France, no. 70204/01, § 53, 12 June 2007), whatever the content of the correspondence concerned (ibid., § 54) [the text of §§ 53 and 54 is available only in French in Hudoc], and whatever form it may take. This means that what Article 8 protects is the confidentiality of all the exchanges in which individuals may engage for the purposes of communication.

Here, and more recently in M.N. and others v. San Marino, the ECtHR clearly stresses a content- and actor-agnostic protection for the confidentiality of private communications.

321 ECtHR Christine Goodwin 2002, para. 74.
322 Steenbruggen 2009, p. 54.
323 ECtHR Michaud v. France 2012, para. 90. See also, more recently, ECtHR M.N. and others v. San Marino 2015, para. 52.
The *CJEU Digital Rights Ireland* ruling connects communications security to the new article 8 EU Charter on data protection.\(^{324}\) Voicing concerns over conceptualizing communications security protection through data protection may seem like a somewhat academic debate. However, section 3.2 of this study pointed at the drawbacks of conceptualizing communications security as a data protection issue: the definition of ‘personal data’ is subject to intense debate in the ongoing revision of the data protection framework; the possible introduction of a new category of ‘pseudonymous data’ and the fact that personal data is just a subset of the information and communications that traverse global networks. Data protection lawmakers may not be aware of the impact of their decisions beyond data protection because of these links to other policy cycles. Possibly, policymakers believe all fundamental rights values have been ‘covered’ because of a cross-reference to data protection law.

Fundamentally, data protection will increasingly fail to protect communications security in the networked environment. De Hert & Gutwirth coin two functions of privacy, which are briefly summarized here to point at the limitations of data protection as a conceptual anchor. Privacy can be seen as a tool for ‘opacity’ and ‘transparency’.\(^{325}\) Opacity is the classic conception of ‘shielding’ a broad range of practices from intrusion. One of the straightforward tools to ensure opacity is prohibition by granting rights even a user cannot waive. Obviously, such prohibitions are not absolute, but when opacity is found vital it can only be broken through strict limitations tests, such as the ‘necessity in a democratic society’ test under ECtHR law. Rather than opacity, privacy can also be treated as a tool for ‘transparency’. Transparency aims to ensure ‘fairness’ of data flows, primarily through procedural safeguards such as consent. Seen in this way, users become transparent through the flow of data, and inherent power

\(^{324}\) See section 4.2.
\(^{325}\) De Hert & Gutwirth 2006.
imbalances in data flows are corrected by observing some basic criteria in the process.

Data protection is primarily a transparency tool. It has some opacity capacities: some data flows are forbidden, such as certain prohibitions when it comes to sensitive data. But in general, Gutwirth & De Hert critique data protection as increasingly losing its normative ‘opacity’ capacities in the last decades. Even as a tool for transparency EU data protection has become too ‘proceduralized’, up to the point that it has lost its normative capacities of fairness, Gutwirth & De Hert argue. Other scholars have also critiqued data protection for relying too heavy on procedural safeguards; users usually just waive to get access to a service. Borgesius argues that increased user protection is needed in data protection and recommends opacity tools to do so. Koops has even called data protection a “zombie” and wonders what to do with a dead body of law that has increasingly become meaningless in protecting users today.

Conceptualizing communications security as data protection runs into similar risks, and De Hert & Gutwirth argue that next to the home, correspondence deserves firm opacity protection through fundamental rights law. Data protection is in itself incapable of achieving a firm constitutional stance on protecting communications where this may be due. The next sections will study more closely the specific fundamental rights value of communications secrecy as a conceptual source for communications.

A Functional Approach for Scoping Communications Security

---

326 Zuiderveen Borgesius 2014.
327 Koops 2014.
328 De Hert & Gutwirth 2006.
Sprawling innovations in communications technologies over the last decade have already led the ECtHR to adapt, adopt and improve fundamental rights protection with regard to new communication technologies. Generally, the Court calls for a “dynamic and evolutive” interpretation of the ECHR to mitigate the risk of fundamental rights law being a bar to reform or improvement:”

*It is of crucial importance that the Convention is interpreted and applied in a manner which renders its rights practical and effective, not theoretical and illusory. A failure by the Court to maintain a dynamic and evolutive approach would indeed risk rendering it a bar to reform or improvement (...).*

Already in 2004, the ECtHR observed that “increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data.” Internet communications have been brought within the scope of article 8 ECHR in 2007. In *ECtHR Copland v. The United Kingdom*, after noting that telephony already fell within the scope of article 8 ECHR, the ECtHR quite easily held that “it follows logically that e-mails sent from work should be similarly protected under article 8, as should information derived from the monitoring of personal Internet usage.” Adding the word ‘logically’ is apparently enough for the ECtHR to dynamically apply its living instrument doctrine.

In July 2013, the ECtHR expanded the scope of the fundamental rights protection of the Convention to all data on a ‘cloud’ server, regardless of

---

330 ECtHR Christine Goodwin v. United Kingdom 2002, para. 74. See also ECtHR Armonas v. Lithuania 2008, par. 38.
331 ECtHR Von Hannover v. Germany 2004, para. 70.
332 ECtHR Copland v. United Kingdom 2007, para. 41. Emphasis added.
333 With similar flexibility, GPS monitoring was afforded constitutional protection in ECtHR Uzun v. Germany 2010.
whether that data in effect identifies a (legal) person or not. The Norwegian government had mandated the applicants:

“to provide access to and enable the tax auditors to take a copy of all data on a server used by all three applicant companies (...) The imposition of that obligation on the applicant companies constituted an interference with their “home” and undoubtedly concerned their “correspondence” and material that could properly be regarded as such for the purposes of Article 8.”

As such, the data that relate to ‘cloud’ computing communications fall under the scope of the respect for correspondence, regardless of whether these data are ‘personal data’ or not. The aforementioned Michaud v. France and M.N. a.o. v. San Marino rulings of the ECtHR extend article 8 ECHR unambiguously to the protection of “the confidentiality of all the exchanges in which individuals may engage for the purposes of communication”, regardless of the content communicated or the means of communication. Another question yet to be dealt with by the European fundamental rights courts is whether communications secrecy extends to our communications devices. So far, constitutional courts around the world that have had the opportunity to rule on the issue have also firmly established communications devices deserve extensive fundamental rights protection. In June 2014, the US Supreme Court issued a landmark ruling in Riley v. California in which it established that mobile phones must be afforded strong constitutional

334 ECtHR Bernh Larsen Holding and Others v. Norway 2013, para. 106. See also para. 163. The case concerned the request of an entire ‘cloud’ server for the purposes of a tax investigation. As taxation lies at the core of a national governments public services, and the Norwegian tax authorities took significant steps to safeguard the access to those data against abuse by the authorities, the Court granted Norway a large margin of appreciation and held no violation of article 8 ECHR. The Court also granted a wider margin of appreciation because the complaint was not brought by an individual, but by a company (para. 159). Apart from a sharp dissenting opinion, the majority of the Court held that in other spheres of government activity – notably law enforcement (para. 173) – its proportionality test would have been much stricter and less margin of appreciation would have been granted to a Member State.

335 ECtHR M.N. and others v. San Marino 2015, para. 52
protection. In 2008, the German Constitutional Court even created a new constitutional right in the ‘confidentiality and integrity of IT-systems’ in a case involving the admissibility of criminal law regulating active hacking by government authorities, through remote searches of IT-systems using Trojan malware (‘Bundestrojaner’). The current conceptualization of communications security in the German Constitution, which only contains an explicit protection for the “house” (article 13.1 German Basic Law) and for “telecommunications” (article 10.1 German Basic Law), did not sufficiently protect citizens in the networked communications environment. The German Constitutional Court did not precisely define which ‘systems’ fall under the scope of the right, and only mentioned that non-connected devices that only store data marginally relevant to constitutional rights do not fall under its scope. The mere ability of interconnectivity and storage capacities was found sufficient, and computers, laptops, smartphones and electronic calendars were named as examples of IT-systems that are covered by the new ruling – regardless of whether these systems actually contain sensitive personal data.336

Both rulings hold that communications devices can harbor a startling amount of sensitive communications and data on both the communicant and third parties, as well as often being connected to cloud servers beyond the device. Therefore, both constitutional courts rule that communications devices need to be afforded constitutional protection that exceed the protection of the home and narrow conceptions of telecommunications.337 It is highly likely that the ECtHR will deploy its “living instrument” doctrine to extend the protection of communications secrecy to communications devices and follow the reasoning in the German and US case law when confronted with an application, as it has done to cloud computing with the aforementioned 2013 case *ECtHR Bernh Larsen Holding a.o. v. Norway*. With regard to the Bundestrojaner ruling, for

example, Groothuis & De Jong established that many of its elements already find resonance in ECtHR case law.338

New socio-technical realities make the current approaches to scoping ‘communications security’ in EU legislation even more unsustainable. With regard to online security technologies, Hildebrandt has argued that “coming to terms with freedom infringements requires that we take serious the security issues generated by the cocktail of an exponential increase (1) in remote control, (2) scale and (3) speed, (4) hyper-connectivity and (5) automation” that change “the mode of existence of fundamental rights such as privacy, data protection, non-discrimination, due process and free speech.”339 Beyond the intelligence surveillance operations disclosed by Snowden, section 3.2. already provided the data breach notification, Phorm, the omission of private key storage around digital certificates and STARTTLS downgrade attacks as practical examples of the drawbacks of rigid conceptualization around ‘scope’ and ‘personal data’, in defense of more open approaches to protect communications security.

Such open approaches for EU legislation should be informed by European fundamental rights law that adopts a functional approach: aforementioned ECtHR case law holds that a basic level of fundamental rights protection needs to be afforded, agnostic to which ‘actor’ or ‘technology’ is used or whether ‘personal data’ is involved. The ECtHR is deliberately reluctant to define the concept of ‘privacy’ and ‘correspondence’, opting for flexibility when faced with technological turbulence through its “living instrument” doctrine. In addition to the ECtHR, the EU legislature itself has long observed the need for dynamic, evolutive, and functional approaches to EU communications law. In a 1999 Green Paper on “The Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation”, the

338 Groothuis & De Jong 2010.
339 Hildebrandt 2013, p. 358.
EU Commission already observed the need to regulate communications infrastructure and services equally, regardless of the transported information. With regard to both general scoping issues in EU communications law and its implications for communications security, that vision has never materialized, as observed in Part I. One can speculate as to the reasons why such EU statutory law has become a ‘bar to reform or improvement’, to paraphrase its own words in 1999: perhaps a lack of imagination, expertise, political incentives, or a tendency to frame broad fundamental rights problems as data protection issues may be at play – or rather a combination of all of these. The following chapters, notably chapter 6, will further examine these underlying reasons. But the living instrument doctrine instructs a re-orientation of current scoping arrangements in EU communications security law in favor of a functional approach. The next section of this chapter will further develop a fundamental rights conceptualization of communications security for EU legislation stepping away from ‘actors’ and ‘personal data’ as conceptual anchors, by analyzing the history and the object of fundamental right to communications secrecy.


Communications security is closely tied to the fundamental right to communications secrecy. Since the ECHR came of age in 1950, article 8 explicitly safeguards the ‘respect for correspondence’ as the foundation of communications secrecy in European fundamental rights law. This section briefly outlines the history, underlying values and the afforded protection of

341 The ECHR and ECtHR do not distinguish much between the two conceptualizations, secrecy and confidentiality, and provides ‘objectified’ protection. At the national level, remarkable differences exist between communications secrecy and communications confidentiality conceptualizations. The debate has been especially intense in discussions around updating the archaic article 13 of the Dutch Constitution that still contains protection of the telegraph. See for example Asscher 2002, Steenbruggen 2009.
communications secrecy and argues that communications security should be conceptualized similarly – as an ‘objectified’ first line of defense – to protect communications against arbitrary interference with their fundamental rights.

The nascence of the fundamental right to communications secrecy stems from systematic surveillance of letters by governments. In 1464, the French King Louis XI was one of the first royals in Europe to establish a postal service, and Cardinal Richelieu’s *cabinet noir* is just one of many legendary examples of systemic communications surveillance by a government. Across Europe, when postal services were established, some private and some by the State, systemic surveillance was commonplace. During the 19th century, especially after the French Revolution in 1791, many nations started to adopt communications secrecy in their national constitutions, independently of whether the state had nationalized mail services or not. In addition, communications secrecy developed from merely a narrow right to secrecy to a responsibility to ensure the security of the communications infrastructure against possible third party interferences with the right to communications secrecy. The same underlying constitutional values have been extended to telecommunications and, as discussed in the previous sections, increasingly in the networked communications environment. Conceptualized as ‘letter secrecy’ first, and ‘communications security’ since, throughout history the emergence of a new communications infrastructure has spurred the extension of a fundamental right to protect communications secrecy.

**Underlying Values**

---

342 The strategic value of communications surveillance had long been recognized, for example by Julius Caesar who a special encryption mode to correspond with military leaders throughout the empire. Bergstra & De Leeuw 2007. See also Marsden 2014.

343 Steenbruggen 2009.


345 See on the history of the legal protection of confidentiality of communications Steenbruggen 2009, p. 11 and Ruiz 1997, p. 64-70.
At the outset the protection of communications secrecy found its rationale in the protection of trade secrets. It was only later that privacy and communications freedom became added fundamental rights and joined the flock. The free flow of information is one of the classic rationales of protecting the confidentiality of communications. The importance of confidential communications for expressive conduct had long been recognized. It protects such individual values as autonomy, the right to receive and impart information, the freedom of thought and anonymity. The absence of communications confidentiality on expressive conduct can cause a so-called “chilling effect”: when in a state of being watched, people tend towards compliance and self-monitoring, rather than thinking, acting and speaking freely. Societal values of communications freedom served by communications secrecy include protection against censorship and the normal functioning of a democratic society. The instrumental value of communications secrecy for a free press and source protection manifests itself clearly throughout ECtHR case law.

Freedom of association is another fundamental right that cannot exist without communications secrecy. A new and as of yet constitutionally unresolved issue, is the particular threat of passive metadata surveillance, with the explicit aim to create a “social graph” of the entire population, to the freedom of association. Metadata in the repositories of Western intelligence agencies are stored, it was revealed, for five years by default. The constitutionality of such complete

350 ECtHR Voskuil v. The Netherlands 2010.
351 Strandburg 2008.
352 Extensively discussed in Arnbak & Goldberg 2015.
associational mapping through metadata operations revealed by Mr. Snowden is currently been debated both in US courts and soon before the ECtHR and CJEU. The protection of article 8 ECHR also extends to searches at corporations. Thus, we see that a broad range of constitutional values are served by the fundamental right to communications secrecy.

An 'Objectified' First Line of Defense

Communications secrecy affords broad protection, before it is clear to what extent fundamental rights are infringed upon. In ECtHR case law, communications secrecy can be seen as agnostic to context and intent. This has been made clear in several cases before the ECtHR. In a case regarding a wiretap and undercover operation targeting a drug dealer, the ECtHR applied different criteria to assess whether the ‘respect for correspondence’ had been violated under article 8, than to assessing a possible violation of the ‘respect for the private life’. The Court reasoned that the drug dealer knowingly committed crimes and thus it applied less scrutiny to the alleged violation of the respect for his private life. However, the infringement on the ‘respect for correspondence’ was scrutinized thoroughly. The ECtHR has ruled similarly with regard to professional secrecy. Before looking into the lawyer-client relationship, the ECtHR considered the infringement of article 8 ECHR as a breach of communications secrecy. Similarly, in ECtHR Craxi II a former Italian Prime Minister was legitimately investigated for alleged corruption, but

353 CJEU C-362/14 (Schrems v. Data Protection Commissioner) 2015 (ongoing). Note the differences with constitutional law in the United States, where the so-called third party doctrine has the exact opposite effect. As soon as a communicant makes use of the services of an intermediary, the US constitutional law holds that a user loses out on his reasonable expectation of privacy. See Van Hoboken, Arnbak & Van Eijk 2012.
354 ECtHR Colas Est 2002, para. 40-42.
355 ECtHR Lüdi 1992.
356 ECtHR Kopp 1998, para. 72.
the disclosure of completely private data irrelevant to the investigation to third parties was deemed a breach of the “respect for correspondence.”

Nieuwenhuis has called the “respect for correspondence” under article 8 ECtHR a “first line of defense” for other fundamental rights. Regardless of the content, context or intent of the communications, the mere use of communications deserves objectified protection. The core theory behind the concept is that it serves as a first line of defense for communicants, that entrust their communication to an intermediary, and thus lose control over its disclosure both to the intermediary and possible third parties. This dependence has constituted the principal rationale for the protection of communications secrecy. In framework of Gutwirth & De Hert, communications secrecy under ECtHR case law serves as a tool for ‘opacity’, rather than the ‘transparency’ of ‘personal data’ protection.

Communications secrecy could be conceived of as a proto-fundamental right, standing as the first line of defense between arbitrary intrusion on communications and the enjoyment of fundamental rights. The first line of defense extends beyond the communications channel, even beyond the point where the intermediary effectively controls the communication. In ECtHR Niemietz the Court did not only extend the reach of the “private life” to corporations when their premises are raided by the government, but unopened letters already delivered to the company involved also fall under the protection of communications secrecy.

*Communications Secrecy and Security vis-à-vis Positive Obligations*

---

357 ECtHR Craxi II 2003. It follows that once the transcripts were deposited under the responsibility of the registry, the authorities failed in their obligation to provide safe custody in order to secure the applicant’s right to respect for his private life.


Communications secrecy implies both an *a priori* prohibition of communications intermediaries against taking notice of the communications, as well as an insistence on protecting the communicant against unauthorized disclosure to subcontractors or third parties including governments. In other words, this concerns negative and positive rights in both vertical and horizontal relations.

In the 1990s, the vertical relationship has already been recognized with regard to electronic communications. The interception article of the CoE Cybercrime Convention, aimed at criminalizing interception of communications and regulating wiretapping, is one of the central provisions in European law to establish positive obligations to regulate communications secrecy of end users in vertical relationships. 360 And the ECtHR has a substantial body of case law on the matter, for example, the 1997 *ECtHR Halford v. The United Kingdom* case regarding the wiretapping of an employee of the UK police by her employer. 361 The explanatory memorandum of the Cybercrime Convention explicitly mentions *Halford*, and further mentions five ECtHR court cases to point at the constitutional dimension to criminal law approximation in this space to safeguard against abuse of power. 362

Along with negative rights, Steenbruggen has extensively researched positive rights to communications secrecy under article 8 ECtHR, and made the following schematic representation: 363

---

360 Discussed in section 2.5. It had already been proposed in the 1989 Recommendation as deserving protection, see Council of Europe, *Computer-related Crime*, Rec. R (89) 9, 1989, p.53.
361 ECtHR Halford v. United Kingdom 1997.
Steenbruggen paints a comprehensive picture with regard to positive rights to communications secrecy. Notably, Steenbruggen includes communications security measures as positive obligations; both with regard to direct state conduct and indirect state conduct, meaning mandates to private sector actors through legislation. While the CJEU had not yet established positive rights with regard to communications secrecy at the time the figure was designed, Steenbruggen and De Hert have both argued that the E-Privacy Directive at the time effectively met the requirements of the ECtHR at the EU level.  

According to this view, the EU lawmaker intended to establish positive rights requirements under the ECHR and protect communications confidentiality, both in vertical and in horizontal relationships.

---

But socio-technical realities rapidly change over time. Limiting the scope of the fundamental right to communications secrecy to communications ‘in transit’ or ‘personal data’ fails to meaningfully protect private communications in the current networked communications environment, where ‘cloud’ computing and ‘smart devices’ belong to dominant communications uses. The ‘actor’-based scoping problems persist in the E-Privacy Directive – limited to conventional telecommunications operators – even if privacy regulators such as the Article 29 Working Party stretch the scope of the E-Privacy Directive to include ‘personal data’ processing, as noted in Part I. Moreover, it seems the EU lawmaker itself has not departed from the ‘actor’-based scope approach in the E-Privacy Directive in its recent legislative action, by extending these positive obligations to protect against unlawful disclosure beyond the Telecoms Package following a functional approach; as can be witnessed from recently adopted laws such as the eIDAS Regulation and debates in the Network and Information Security Directive. Part I concluded that the European end user is left with a highly fragmented patchwork of protection. As observed in the previous section, the ‘living instrument’ doctrine of the ECtHR suggests a broader, more functional scope of ‘communications’ and thus an extension of communications secrecy beyond communications in ‘transit’.

The combination of these socio-technical developments, the Snowden disclosures and a surge in cybercrime have demonstrated an aggressiveness of CoE Member States, cybercriminals, advertising networks and a wide array of third parties in vertical and horizontal relationships alike to breach basic fundamental rights. To uphold ‘practical and effective’ fundamental rights protection, legal ‘procedural’ approaches need to be complemented with technological safeguards. As the ECtHR has held in a number of cases, the means of communications themselves deserve protection as interferences with

the means necessarily interfere with fundamental rights guaranteed by the ECHR, including communications freedom. Technical security measures seem essential to ensure broader fundamental rights protection.

Conversely, robust technical security cannot and should not obscure broader fundamental rights evaluation. In *ECtHR M.K. v. France*, the Court provided some clarity on the relationship between data security and other fundamental rights. The case concerned the French fingerprint database FAED, which collected biometric data on all French citizens ever subject of a law enforcement investigation. The database kept these data for 25 years, regardless of suspicion in ongoing investigations. Moreover, the design of the database implies “the purpose of the database, notwithstanding the legitimate aim pursued, necessarily involves adding and retaining as many names as possible.” France’s view that fundamental rights were protected through applying data processing safeguards and holding onto the fingerprints to protect citizens against identity theft fails under article 8 ECHR. In confirming *S. and Marper v. The United Kingdom*, the Court considers that accepting the argument based on an alleged guarantee of protection against potential identity theft would in practice be tantamount to justifying the storage of information.

---

366 See for example ECtHR Autronic AG v. Switzerland 1990. In similar vain: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 22 May 2015, para. 56-60: “Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. (...) States should adopt policies of non-restriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective, require court orders for any specific limitation, and promote security and privacy online through public education. (...) Blanket prohibitions fail to be necessary and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows.” Another U.N. Special Rapporteur agrees: “there is a risk that systematic interference with the security of digital communications will continue to proliferate without any serious consideration being given to the implications of the wholesale abandonment of the right to online privacy.” See U.N. Special Rapporteur On The Promotion And Protection Of Human Rights And Fundamental Freedoms While Countering Terrorism, A/69/397, 23 Sept. 2014, para. 14.


368 ECtHR M.K. v. France 2013, para. 36.

369 ECtHR M.K. v. France 2013, para. 25.
on the whole population of France, which would most definitely be excessive and irrelevant.”\textsuperscript{370} In a 2013 case on the monitoring of employee working environment conditions, the CJEU also held that article 17 of the Data Protection Directive does not, in and of itself, negotiate the authorization of access to certain data. The data security provision safeguards, technically, that data access is limited to those entities that enjoy – on legitimate grounds – authorization to do so.\textsuperscript{371} Consequently, the view\textsuperscript{372} that it suffices to protect data security interests of users without proper safeguards against overbroad or illegitimate collection or access conditions does not satisfy the European courts.\textsuperscript{373}

The extension of communications secrecy beyond communications ‘in transit’, technical safeguards along with legal safeguards as well as the relationship between communications secrecy, communications security and broader fundamental rights will be further explored in following sections and the case studies of Part III on HTTPS and ‘cloud’ communications.

\textbf{4.5. Protection Against Arbitrary National Security Interferences}

Part I of this study showed how communications security is a crucial issue in a broad range of policy areas, such as consumer protection, E-commerce, protecting citizens against various forms of cybercrime and E-Government. In addition, Part I found that national security has played a major role in EU communications security law- and policymaking since its very advent, and long

\begin{flushright}
\textsuperscript{370} ECtHR M.K. v. France 2013, para. 41
\textsuperscript{371} CJEU C-293/12 and C-594/12 (Digital Rights Ireland a.o.) 2014, para. 28-29.
\textsuperscript{373} See for instance ECtHR S. and Marper v. The United Kingdom 2008, para. 122, in which the Court held that mere retention of biometric data for the purposes of law enforcement constitutes a violation of article 8[1] ECHR and reflects on the risks of stigmatization and the presumption of innocence.
\end{flushright}
before too. Explicit, implicit and secret national security influences were identified, along with competence complexities for the EU lawmaker to regulate communications security as soon as national security comes into play. Clearly, the interplay between communications and national security is a vexing issue that cannot longer be denied or shied away from by the EU lawmaker in seeking solutions to secure private communications through EU law. This section does not comprehensively review ECtHR national security case law, but rather explores how national security relates to communications security from a constitutional perspective.

The ECtHR’s Legal “Safeguards Against Arbitrary Interference”

The classic parameters for limiting fundamental rights of article 8[2] and 10[2] of the ECHR are also assessed in cases on national security: surveillance regulations must meet “quality” requirements (be clear, specific, accessible) to be “provided by law”, be “necessary” and “proportionate to the legitimate aim pursued” and “effective remedies” and “supervision” must be in place. ECtHR case law does recognize national security as one of the central ‘legitimate aims’ to limit constitutional protections afforded by the Convention. A general yardstick in ECtHR case law, developed in the 1978 ruling ECtHR Klass a.o. v. Germany, is whether secret surveillance “entails the risk of undermining or even destroying democracy on the ground of defending it”. In 1978, that meant not ruling void strategic monitoring a priori, but demanding legal safeguards against arbitrary interference. In 2006 a well-organized German system of strategic monitoring of telecommunications was not considered in breach of the Convention, whereas less regulated British and Moldovan

---

377 ECtHR Weber and Saravia v. Germany 2006, para. 94.
systems were found to violate article 8 ECHR for a lack of safeguards against abuse of power in 2008 and 2009 respectively.\textsuperscript{378}

Of these two cases, ECtHR Liberty a.o. v. The United Kingdom seems particularly relevant to the ECtHR’s stance with regard to safeguards against national security overreach.\textsuperscript{379} In 1999, a TV show disclosed the existence of the Electronic Test Facility (“ETF”) at Capenhurst in Cheshire, operated by the UK Ministry of Defense. Here, all electronic communications between the British Isles was intercepted and analyzed in bulk. Soon afterwards, Liberty, the Irish Council for Civil Liberties and several other British NGOs launched a case against the UK government. The NGOs had provided legal advice to activists during the 1990s and had legitimate concerns about being victims of the reported systematic mass surveillance of all telecommunications across the British Isles. The facts and the ECtHR’s evaluation of the British legislation that regulated the surveillance seem similar to several operations disclosed by Snowden:\textsuperscript{380}

\begin{quote}
The 1985 Act [on which the UK government based its surveillance program] allowed the executive an extremely broad discretion … virtually unfettered; for example, all commercial submarine cables having one terminal in the UK and carrying external commercial communications to Europe; Information could be … listened to or read, if the Secretary of State considered this was required in the interests of national security, the prevention of serious crime or the protection of the United Kingdom’s economy; material was selected for examination by an electronic search engine, and search terms, falling within the broad categories covered by the [surveillance order] certificates, were selected and operated by officials.
\end{quote}

The Court struck the surveillance practices down for not being ‘in accordance with the law’. In other words, the legislation on which the British Government

\textsuperscript{378} ECtHR Liberty and Others v. the United Kingdom 2008, para. 62. ECtHR Iordachi and Others v. Moldova 2009.
\textsuperscript{379} For an discussion of the case, see Ambak 2014b.
\textsuperscript{380} ECtHR Liberty and Others v. the United Kingdom 2008, para. 64-66.
based its untargeted surveillance was so vague and ambiguous that it didn’t meet the *procedural* requirements for surveillance laws under the ECHR – thus constituting a violation of Liberty’s privacy rights. Failing to meet the first *procedural* test, the Court was able to avoid the politically sensitive, *substantive* test, i.e. whether the 1990s ETF program was ‘necessary in a democratic society’.

So far, the general case law of the ECtHR seems to opt for legal safeguards on the procedural level, and a margin of appreciation for Member States when it comes to the substantive level. Nations regulate national security as long as law exists to legalize such secret surveillance. As a consequence, the ECtHR had developed a casuistic stance towards national security case law, emphasizing legal ‘procedural’ safeguards, rather than substantial ones. As such, reminiscent of the framework offered by Gutwirth & De Hert, the ECtHR seems to have generally opted for a quite limited ‘transparency’ of power approach through demands on legal bureaucracy, rather than ‘opacity’ of the individual through meaningful protections. In specific cases, the transparency approach is complemented with elements of opacity in contexts towards which the ECtHR takes a more sensitive stance, for example on source protection for journalists.

In the upcoming Snowden cases, discussed below, it seems unlikely the ECtHR will be able to fully base its ruling on an assessment of procedural legal safeguards. Several legal and political puzzles exist, however, for the ECtHR to substantively assess national security overreach. A first puzzle is the unclear margin of appreciation in the mass surveillance operations disclosed by Snowden and challenged by these NGOs. The substantial insight of the general public into these operations is historically unparalleled. If the Court rules that

381 See for example ECtHR Telegraaf Media Nederland Landelijke Media B.V. a.o. v. The Netherlands 2012.
the procedural legal safeguards are met, it has to move onto substantive assessment given the facts that are on the table. To what extent is the ECtHR ready to evaluate operations such as PRISM and TEMPORA, in light of earlier rulings that surveillance must not “destroy democracy on the grounds of defending it”? Who gets to decide the conception of ‘democracy’ in these highly controversial areas: the ECtHR or the nation state? The extent of the margin of appreciation in general is tied to a second, more specific puzzle: national security is often invoked as a legitimate ground for deviating from fundamental rights protection ensured by the ECHR, but it lacks a proper definition in the ECHR and in the ECtHR case-law. Privacy is the rule, national security the exception. But what falls under the exception is unclear, and often regarded as a state secret. It has become clear that national security serves as a fruitful concept to legitimize covert government surveillance in areas as diverse as economic espionage, agriculture or climate change policymaking. Has the exception become the rule? And will the ECtHR provide a definition of national security in the upcoming cases, or leave it to nation states to define national security? The CoE Commissioner for Human Rights recently called for leadership of the CoE and the ECtHR in this area. The coming years will most probably provide answers to these vexing questions.

A Case for Legal and Technical Safeguards Against Arbitrary Interference

The coming years will see a number of highly relevant cases considered by the ECtHR. Some of them, such as 

ECtHR Zakharov v. Russia, 383 will most

382 Council of Europe Commissioner for Human Rights 2014.
383 An early indication of whether the ECtHR will adapt its classic examination of communications surveillance may come in the Grand Chamber ruling in ECtHR Zakharov v. Russia, no. 47143/06 (ongoing), for which the Grand Chamber held a hearing on 24 September 2014. But the case concerns secret surveillance of a leading Russian journalist by the Russian intelligence agency FSB, based on an unpublished FSB policy, which most probably will fail to meet the “quality of law” requirements. A date for the final judgment was not known at the time of conclusion of this research. See <http://hudoc.echr.coe.int/webservices/content/pdf/003-4879141-5963073>, accessed 2 September 2015.
probably be ruled along aforementioned lines as lacking legal safeguards. Others, notably a handful of initiated cases on the national level that have already been launched in reaction to news reports based on documents released by Edward Snowden, may prompt the ECtHR to develop case law on technical safeguards in addition to legal safeguards in the sphere of national security. Two cases initiated by the British NGO Privacy International seem of particular interest. In response to a range of Snowden disclosures – amongst others the QUANTUM, TURBINE, INCENSER and DREAMY/TRACKER/NOSEY SMURF operations – on hacking of communications hardware software and protocols of millions of end-user devices a case has been initiated to challenge these practices.\textsuperscript{384} A second case concerns implications for fundamental rights of active hacking of Internet Service Providers’ infrastructure across the EU and was launched jointly by Privacy International and a group of ISPs.\textsuperscript{385} The latter case has become even more relevant in light of recent news stories on pervasive hacking by the GCHQ of Belgian ISP Belgacom through employing advanced malware known as \textit{Regin} that presents itself as legitimate Microsoft software. Upon publication by antivirus vendor Symantec in November 2014, the malware has slowly but surely been found across computer systems such as those of the European Commission and European Parliament\textsuperscript{386} and large GSM networks.\textsuperscript{387}

At this point in time, one cannot descriptively establish how the ECtHR will rule in aforementioned cases underway to the ECtHR in response to Snowden’s

disclosures. Historically, especially in ECtHR case law and when national security is at stake, the road towards positive obligations to afford constitutional protection is taken on a case by case basis. Still, since ECtHR Liberty a.o. v. The United Kingdom some developments may point towards stricter fundamental rights protection: the ECtHR seemed keen on fast-tracking some of these cases; the CoE Commissioner for Human Rights sharply criticized the current status quo in a widely discussed December 2014 report, and the CoE Conference of Ministers adopted Resolution No. 1 that invites, amongst other references to the Snowden revelations, the Council of Europe to quickly address questions on mass surveillance, backdoors and other ways of weakening encryption systems. The three developments combined indicate that the issues are taken seriously by various institutions at the CoE level, prompting a response from the ECtHR when several initiated cases arrive at the ECtHR in due course.

From a normative standpoint, the time seems long overdue for the ECtHR to revisit the conventional approach to satisfy itself with generalized legal ‘procedural’ safeguards. The positive obligations developed in both ECtHR I. v. Finland and CJEU Digital Rights Ireland should not be limited a priori to accommodate national security inferences and can, moreover, play a valuable role in protecting citizens against arbitrary interferences by national security...

388 See Arnbak 2014c. The initial fast-tracked procedure was based on earlier findings in ECtHR Kennedy v. The U.K. in which the Investigatory Power Tribunal (‘IPT’) in the U.K. was not held to provide an “effective remedy”. However, it was withdrawn several months later, when the U.K. government conceded additional safeguards for a fair trial on the national level which led the ECtHR to decide that ensure domestic remedies had to be exhausted first. Meanwhile, in another case on the same surveillance disclosures, the IPT has held that the GCHQ’s conduct of mass surveillance on fiber-optic cables in ‘legal in principle’, but still has to decide whether TEMPORA was justified and proportional after another round of submissions during a secret, closed hearing. The NGO’s have responded they will appeal the decision at the ECtHR, regardless of the outcome at the IPT. The latest information is available at <https://www.privacyinternational.org/legal-actions>, accessed 2 September 2015.

389 Council of Europe Commissioner for Human Rights 2014.

390 Council of Europe, Freedom of Expression and Democracy in the Digital Age Opportunities, rights, responsibilities, 8 Nov. 2013, Resolution no. 1., para. 13 (v).
agencies, cybercriminals, corporate actors and whomever seeks to attack private communications. No ruling of the ECtHR or CJEU currently obstructs robust technical measures to serve constitutional protection, not even in the sphere of national security where secret surveillance has been conventionally allowed. Moreover, fairly straightforward technical measures seem to be available to make so-called dragnet, bulk, mass or untargeted surveillance cost-prohibitive and thus serve as an ‘objectified’ first line of defense. Some of them have been adopted by major market actors in response to Snowden’s disclosures. These observations are further explored in the case studies of chapters 8 and 9.

4.6. Legislatures’ System Responsibility to Protect

All developments combined seem to indicate a trend towards comprehensive positive obligations to protect communications security in EU law. With the serious wording in the landmark cases of the ECtHR and CJEU discussed in section 4.2, European courts seem to increasingly demand from legislatures to ensure and enforce communications security for end users. In ECtHR I. v. Finland and CJEU Digital Rights Ireland, the courts explicitly point at the relevant legislature to make a normative extension of existing constitutional case law and theories.

In 2012, De Hert argued that legislatures have a “system responsibility” to protect electronic communications security, and that the ECtHR and the CJEU will hold legislatures accountable for its protection. Constitutional courts will increasingly analyze if sufficient efforts have been taken to protect communications security, and prevent breaches. This will particularly be true in cases that cover the CJEU Digital Rights Ireland parameters sensitivity,

391 De Hert 2012, p. 9.
quantity and risk of abuse. Hildebrandt offers a similar framework: “the seriousness of a threat or vulnerability will depend on the expected frequency of the violation of confidentiality, integrity and/or availability and its impact. Ranking the impact will depend on the amount of individuals who will be affected, the distribution of the impact, the invasiveness, duration and secondary effects.” If such factors are at stake, the EU lawmaker should assume system responsibility and legislate communications security from a constitutional perspective.

Probably, the system responsibility of legislatures will only increase over the next years. Following the wording of the CJEU, communications generally have become more sensitive, increased in scale and the risk of abuse has grown as we depend on a myriad of communications providers beyond conventional ISPs to mediate our communications. Users will increasingly depend on their providers and lawmakers to secure their communications. As ever, surveillance is probably on the rise. Bankston & Soltani present basic calculations to highlight the falling costs of surveillance in the networked environment. Inspired by the US Supreme Court in US v. Jones, they argue that even if the desire of the state has always existed to intercept and analyze all communications, the costs were simply prohibitive until relatively recently. Benkler has made similar claims and argues that widespread surveillance enabled by the networked environment has detrimental effects on the affordances of and constraints on freedom. If these dynamics are not responded to by positive rights, the constitutional first line of defense evaporates in the face of the ‘increased vigilance’ demanded by the ECtHR with regard to new communications technologies. The case studies of Part III

392 See section 4.2.
393 Hildebrandt 2013, p. 361.
394 Bankston & Soltani 2014.
will delve into these observations with regard to specific communications technologies and relatively new use cases: HTTPS and ‘cloud’ communications.

Finally, even if legislatures have a system responsibility to protect based on a constitutional perspective, it doesn’t automatically follow that legislatures comply with it. Following *CJEU Digital Rights Ireland*, EU Member States have responded in completely mixed ways. Many Member States had already gone through the process of repealing the national legislation implementing the Data Retention Directive; some Member States immediately announced plans to repeal national implementation laws of the Data Retention Directive, others argued that their specific national implementation law did not breach the CJEU ruling, and saw civil society actors successfully sue their respective governments to repeal national legislation.396 Even after *CJEU Digital Rights Ireland*, one European Commissioner announced plans for a new Directive, while another denied the plan. The European Commission, generally, has not launched court proceedings against any of these Member States for maintaining data retention schemes that are non-compliant with *CJEU Digital Rights Ireland*.397 Meanwhile, the United Kingdom has continued and broadened data retention schemes, controversially basing its actions on its national margin of appreciation. In other words, a legal obligation resulting from a case before the European courts doesn’t automatically translate into action on the national law- and policymaking level. The apparent strong political incentives to maintain controversial surveillance measures that put severe pressure on fundamental rights are the subject of chapter 6, which studies political perspectives on communications security.


4.7. Conclusion

From a fundamental rights perspective, communications security should be conceptualized as an ‘objectified’ first line of defense to protect against unauthorized breaches of the fundamental rights values underlying the c.i.a.-triad. With the emerging constitutional recognition for technical security as a negative and a positive right, and in vertical and horizontal relationships, protecting communications security has become a constitutional requirement, and will be increasingly strictly scrutinized. Theories on establishing positive obligations and limiting protection under the ECtHR can serve as a conceptual anchor for how to establish this ‘objectified’ constitutional first line of defense for specific communications functions. Particularly, the fair balance test for positive obligations could be combined with CJEU Digital Rights Ireland. This landmark case annulled the controversial EU Data Retention Directive and provided a clear conceptual framework to assess when legislative rulemaking beyond market considerations is required to ensure “full” communications security. Fundamental rights oblige the EU lawmaker to provide strict legal guidance when a specific legislative debate touches upon three factors: information sensitivity, quantity and risk of abuse.

The ECtHR has observed that “increased vigilance” is needed to protect fundamental rights in the networked environment. This increased vigilance will likely become more pronounced when legal proceedings initiated in the wake of the Snowden revelations will be treated by the ECtHR. Of particular note are a case on the implications for fundamental rights of bulk surveillance of seemingly unrestrained wiretapping of submarine fiber-optic cables, a case on active hacking of Internet Service Providers’ infrastructure across the EU, and a case on active hacking of communications hardware, software and protocols.
of millions of end-user devices. The ECtHR has shown eagerness to rule on the cases by initially fast-tracking the PRISM case, but when the UK Government satisfied several procedural requirements, it allowed the case to come before the national UK court first. It may take years before delivering these judgments, but the cases will further develop the positive human right to communications security on the long term.

The chapter concludes that communications security can serve as an objectified first line of defense to respond to the challenges inherent in the networked environment for fundamental rights, notably communications secrecy, privacy and communications freedom. The constitutional requirements developed in chapter 4 provide the baseline that the EU lawmaker must uphold and apply in specific legislative instruments. EU communications security legislation must fill the void left by two decades in which availability has been prioritized, but communications integrity and particularly confidentiality have been neglected. Also, given the rapid advances in communications technologies, relying merely on the naturally lengthy process of fundamental rights court proceedings to pronounce positive rights will become more and more insufficient to meaningfully protect private communications. Here, the EU lawmaker has an increased system responsibility to pronounce and help develop the positive obligations to secure private communications.
5. Systems Design Perspectives

Law needs clear definitions and conceptual anchors to determine what is and what isn’t covered by its provisions. After a long period of relative calm, the definition of communications security is currently on the policy agenda across Europe. In addition to information, network, and communications security, in particular ‘cybersecurity’ has become a hot term at the moment; proclaimed by consultants as escalating from the IT-department to the boardroom as a top concern. Moreover, the ‘crypto wars’ of the 1990s discussed in Part I seem to have returned on both sides of the Atlantic – with technology companies implementing stronger encryption in consumer products, FBI executives and the British Prime Minister David Cameron calling for mandated backdoors into all electronic communications and fourteen leading computer scientists harshly criticizing such calls in a much covered July 2015 paper “Keys Under Doormats: mandating insecurity by requiring government access to all data and communications”. To address the conceptual ambiguity of the concept of ‘security’, observed in section 3.1, and add theoretical insights to these prominent policy debates, this chapter turns to computer science to provide a systems design and security perspective on how the EU lawmaker should protect end-user communications security. The insights developed in this chapter serve as a theoretical backdrop for the HTTPS and ‘cloud’ communications case studies of Part III.

398 Baldwin et. al. 2011, p. 67
Systems design and security theory has been around for decades. As this chapter will show, it provides a coherent, flexible and useful concept for defining ‘security’: the c.i.a.-triad. Confidentiality, integrity and availability serve as its three central attributes of ‘security’ (section 5.1). As demonstrated in Part I, traces already exist of the c.i.a.-triad in EU law, but it is not coherently applied across the five EU policy cycles. Moreover, the EU lawmaker seems not to fully comprehend the underlying theories and values, nor the implications of employing the c.i.a.-triad in definitions for technical ‘security’. For instance, the c.i.a.-triad requires policies to negotiate the authorizations inherent in the c.i.a.-triad and for balancing the c.i.a.-triads’ properties when the underlying interests compete (section 5.2) and specification of its attributes to become meaningful (section 5.3). Security requirements engineering provides insights into how systems design deals with these challenges. Then, this chapter will briefly reflect on why technical security fails and reflect on four main failure classes: surveillance, users, technology and markets (section 5.4). The latter reason, market failure, is then discussed more at length through the lens of the relatively new and already influential research area ‘security economics’ (section 5.5). The technical countermeasures available to secure communications are not comprehensively discussed in this chapter. These will be discussed in relation to the HTTPS and ‘cloud’ communications case studies of Part III.

5.1. The Technical Conception of ‘Security’: The c.i.a.-Triad

The technical conception of ‘computer security’ has been the subject of academic studies in computer science at least since the 1960s. Obviously, the field has developed in the last fifty years. In those early days, reliability of vast, expensive computer mainframes was the core concern, and the field was aptly

401 For literature on the general technical measures available, see a.o. Anderson 2008.
named ‘computer security’. Standardized and affordable hardware and software led to a rapid deployment of computing in commercial uses in the 1970s. Consequently, the focus of ‘security’ shifted from computers to information systems and the information contained therein. The associated term ‘information security’ is still much in use today, along with the term ‘information assurance’ that was introduced in the late 1990s to appreciate a broader set of goals beyond ‘security’, such as data quality. In contemporary conceptual computer science literature on ‘security’, the two terms sometimes merge into one concept of ‘information assurance & security’.

Early conceptualizations of technical security emphasized confidentiality as a central attribute. With more widespread use of computers and networked communications by enterprises and consumers, other attributes gained in importance. Over the last decades, a consensus seems to have emerged on the three central attributes that make up the technical conception ‘security’: confidentiality, integrity and availability. In the Encyclopedia of Computer Science, Pfleeger defines them as follows:

- **Confidentiality** – assurance that data, programs, and other system resources are protected against disclosure to unauthorized persons, programs, or systems;
- **Integrity** – assurance that data, programs, and other system resources are protected against malicious or inadvertent modification or destruction by unauthorized persons, programs, or systems;
- **Availability** – assurance that use of data, programs, and other system resources will not be denied to authorized persons, programs, or systems.

---

403 Saltzer & Schroeder 1975, p.1278-1308.
404 Cherdantseva & Hilton 2013, p. 546.
These three security attributes lead to the formulation of security goals. Security goals are defined across the literature as ‘general statements about the security of an asset’, aiming to ‘to protect assets from harm’.\textsuperscript{407} An example of a security goal would be: “the government has the integrity goal that financial transactions in a country do not change the total amount of circulating money.” \textsuperscript{408} A security incident arises from a lack, failure, breach of confidentiality, integrity and/or availability of data or other system resources. A ‘vulnerability’ is the existence of a threat that may impact ‘security’ adversely.\textsuperscript{409}

The first traces of the confidentiality-integrity-availability triad (‘c.i.a.-triad’) can be found in 1975,\textsuperscript{410} but its exact formulation is attributed to the Johnson Space Center’s 1989 ‘Pink Book’.\textsuperscript{411} The McCumber’s Cube of 1991\textsuperscript{412} is a useful visual representation of the c.i.a.-triad. Still part of the US National Training Standard for Information Systems Security Professionals,\textsuperscript{413} the McCumber’s Cube provided a first comprehensive overview of information security and its wider engineering and policy environment:\textsuperscript{414}
The c.i.a.-triad can be found in regulation, standards and in technical security research across the globe. Military and intelligence agencies such as the US National Security Agency support it, as well as those parts of the security community motivated by protecting confidentiality interests against those very agencies. This points at both the general acceptance of the c.i.a.-triad as a conceptual framework, and the lack of normative substance of stating or using the c.i.a.-triad per se, as section 5.2. will further discuss. But as a conceptual framework, the c.i.a.-triad is still widely used decades after its inception.

The c.i.a.-triad has been challenged as incomplete in computer science literature. The same attributes are referred to by different names, while the same names are used for describing different attributes. Since 1991, several

---

415 See chapter 2 for examples across E.U. legislation.
417 See footnote 410 for examples.
418 Landwehr 2000. See also Machonachy et. al. 2001, p. 306 (the lead author ‘is with the NSA’, the article reads). On the other hand, see Pfitzmann 2006.
authors have extended the McCumber’s Cube to cover a broader range of interests. In 1998, Parker formulated six attributes that should comprise a technical definition: confidentiality, possession or control, integrity, authenticity, availability and utility. In other work, the c.i.a.-triad has been extended with concepts such as anonymity (non-identifiable data subject), accountability (availability and integrity of a person who performed an operation), non-repudiation (assurance of the accurate sender) and authenticity (accurate identification by a computer system). Auditability (ability to conduct monitoring of all actions) and privacy (obeying privacy legislation and enabling individuals to control personal information) have also been suggested as additional attributes.

Other authors argue that these additional attributes can be subsumed under the c.i.a.-triad. Fabian et al. observe: “accountability and non-repudiation can be classified as integrity goals, authentication as a design mechanism to achieve confidentiality or integrity, and anonymity or un-observability may be subsumed under confidentiality goals.” Auditability is a precondition of integrity, while both assuring auditability and privacy (as well as data protection) may be a priori regulatory and even constitutional criteria of any societal process, and are as such not specifically relevant as ‘security’ attributes. The importance of privacy and broader constitutional criteria is, as we have seen in Part I and chapter 4 of this study, often overlooked in the regulatory conceptualization of ‘security’.

Terms related to ‘security’ appear in the computer science literature, notably ‘assurance’ and ‘dependability’. ‘Information assurance’ expands the scope of the security concept to cover broader interests such as data correctness and data

---

420 Also known as the Parkerian Hexad, first introduced in: Parker 1998.
422 Cherdantseva & Hilton 2013, p. 554.
423 Fabian et. al. 2010, p.12.
In general, one could say the term information assurance is applied to cover the entire information management practice within business.\footnote{Machonachy et al. 2001, p. 307.} From a legal conceptual perspective, these broader interests are addressed as fair information principles under the data protection policy cycle, such as the right to be informed if a data controller holds your personal data, the right to correct those data and so forth. Thus, in this study the concept of ‘security’ is employed: it covers a narrower set of attributes, the c.i.a.-triad, in a broader set of uses (than merely business environments).

Another, older term often encountered in the literature is ‘dependability’. It is defined as the “ability to avoid service failures that are more frequent and more severe than is acceptable”.\footnote{Cherdantseva & Hilton, p. 547.} In general, ‘dependability’ has a broader focus than ‘security’, and includes performance and reliability of computer systems. When these interests are relevant to ‘security’, they can mostly be subsumed under the c.i.a.-triad, particularly the availability attribute. Dependability covers a slightly broader set of attributes than security: availability, reliability, safety, integrity and maintainability. Combined models of ‘security’ and ‘dependability’ have been suggested, integrating the security attributes present in both concepts.\footnote{Avizienis et al. 2004.}

The fact of the matter and of the computer science literature is that decades of academic debate have not actually led to a refined definition of ‘security’. While influential security scholars claim that theoretical approaches to modeling security should serve as ‘guiding example’ for other computer science subareas in the next 50 years,\footnote{Jonsson 2006, p. 646.} on the other side of the spectrum scholars lament such “grand philosophical frameworks” and “settle for a
healthy dose of anti-intellectualism instead.” Schmidt presents what is perhaps the most complete multi-disciplinary conceptualization of “Internet security” known to date, based on the c.i.a.-triad, but immediately realizes characterizes his definition a “conceptual beast”:

Internet security is the low probability of damage to acquired values forming the Internet (such as sub-networks, computing devices, components; integrity, availability, reliability of data) or based and depending on the Internet (such as contents and semantics; economic welfare, autonomy, political independence), which are related to beneficiaries (such as individuals, states, social groups, businesses), with the aforementioned low probability of damages achieved by applying protecting means (either technical, organizational or political in nature) against threats (emerging from either malevolent or ignorant actors, from systemic constellations, technical phenomena or artefacts).

Often, security literature offers a conceptualization close to the c.i.a.-triad and then notes that “a lot of time is spent (and wasted) in trying to define unambiguous notations for security”.

In sum, the underlying interests of secure communications are captured under the c.i.a.-triad, and in the literature other security attributes are often subsumed under the c.i.a.-triad. Many authors now agree that the c.i.a.-triad suffices as a conceptual framework for designing secure systems. The c.i.a.-triad is already in wide use in applied computer science research and to some extent in EU legislation (see Part I), standards and the information security profession. Moreover, the c.i.a.-triad has been referred to in several rulings of European fundamental rights courts. The c.i.a.-triad will thus serve as a basic conceptual framework for communications security policymaking in this study.

430 Schmidt 2014, p. 50-51.
432 See section 4.2.
The next section further develops the c.i.a.-triad and the often conflicting interactions between its attributes.

5.2. The Centrality of ‘Authorization’

The concept of ‘authorization’ is strikingly central to the c.i.a.-triad. If we look at Pfleeger’s definition, confidentiality is breached as soon as a secured asset is disclosed to an unauthorized entity, integrity when an unauthorized entity can modify it, and availability when the authorized entity is denied access to it. Here, ‘entity’ is used as a shorthand for ‘persons, programs or systems’ – Pfleeger’s definition covers humans, software and hardware. The centrality of authorization becomes even clearer from the unified definition of ‘security’ in Avizienis et al: ‘security is the absence of unauthorized access to, or handling of, a system state’.433

Saltzer & Schroeder connect authorization to the notion of control and system constraints.434 From a legal perspective, the immediate questions that arise are how can the centrality of authorization be operationalized, balanced or mediated? Who is this authorized person, how did he or she get authorized, by whom, and who enforces and supervises such crucial decisions?

Pfleeger observes that ‘authorization’ needs to be conferred and subsequently verified through a reliable structure. 435 Such structures include systems engineering (e.g. access control mechanisms), contracts, consent and the legislative process. A key insight is that both in conferring and in verifying

---

434 Saltzer & Schroeder 1975, p. 2: “the term "unauthorized" in the three categories listed above means that release, modification, or denial of use occurs contrary to the desire of the person who controls the information, possibly even contrary to the constraints supposedly enforced by the system.”
435 Pfleeger 2003, p. 505.
authorization, regulation is often an important source for determining authorization.436 We see this all the time. For instance, the European Data Protection Directive has an extensive section on the security of personal data, and so do sector-specific laws in the Unites States such as HIPAA on health data.

The security attributes of the c.i.a.-triad may complement or conflict with each other, depending on the specific communications function used. As Wilson observes: “measures taken to further the goal of one pillar are often blind to the needs of another pillar.”437 One can imagine how availability goals often conflict with confidentiality goals, for instance. This is not unusual for law, where privacy and free flow of information interests often collide, and legislatures or courts are called upon to balance these interests. The c.i.a.-triad can be a valuable tool to conceptualize ‘security’, precisely because it can illuminate such complex interactions.

In its ‘Internet Security Glossary’, the Internet Engineering Task Force (‘IETF’) employs the c.i.a.-triad in its definition of ‘communications security’:438

\[
\text{communication security (COMSEC)} \\
\text{Measures that implement and assure security services in a communication system, particularly those that provide data confidentiality and data integrity and that authenticate communicating entities.}
\]

\textbf{Usage:} COMSEC is usually understood to include (a) cryptography and its related algorithms and key management methods and processes, devices that implement those algorithms and processes, and the lifecycle management of the devices and keying material. Also, COMSEC is sometimes more broadly understood as further including

437 Wilson 2013.
From the IETF definition and additional comment, it becomes clear that the IETF focuses on confidentiality and integrity interests in conceptualizing communications security. Also, the IETF indicates the vital roles of cryptography and key management in securing communications. The case studies of Part III analyze these aspects in detail in specific relation to HTTPS and ‘cloud’ communications.

In essence, the c.i.a.-triad mandates a **procedural operationalization** of authorization. But stating the c.i.a.-triad does not in itself suggest **substantive guidance** for determining authorizations. Security attributes are not verifiable in themselves and do not describe what they actually mean when confronted with a specific communications use, how security goals should be balanced and how conflicting stakeholder interests should be addressed. While the c.i.a.-triad offers a robust procedural conceptual framework, substantive guidance is context specific, and will thus depend on the specific communications use that is subject of either systems design or regulation. In systems design, a class of

---


441 The IETF defines cryptology as follows: $ cryptology (I) The science of secret communication, which includes both cryptography and cryptanalysis. See <https://tools.ietf.org/html/rfc4949>, accessed 2 September 2015.

442 Signal security is a broader term than communications security, including other forms of signals such as radar.

methods known collectively as ‘security requirements engineering’ can help to operationalize the c.i.a.-triad and authorization in specific systems.

5.3. Security Requirements Engineering

The security attributes of the c.i.a.-triad can interact in complex ways, while the centrality of ‘authorization’ in its definition facilitates control or constraint in security policies and systems design. ‘Security requirements engineering’ is a method in computer science employed to illuminate these complex interactions and formulate specific system requirements. ‘Multilateral security requirements engineering’ helps to understand and resolve conflicting stakeholder interests. Both methods provide useful analytical lessons for the conceptualization and legislation of communications security.

Security requirements engineering starts with the observation that merely stating security attributes or goals is not sufficient for any security policy or system. This insight resonates with the historical analysis of Part 1, which found that security definitions are often copied from previous legal documents, without any consideration or guidance on how to balance underlying, and often competing values inherent in legislating communications security. Security requirements engineering seeks to increase the specificity of security policies in systems design, in order to make these policies meaningful. The level of detail

444 This section looks into the specific field of security requirements engineering. For a more general account of systems theory and safety engineering, see Leveson 2011.

445 The Common Criteria (available at <http://www.commoncriteriaportal.org/cc/>) are a well-known method in software engineering to "achieve comparability of independent IT security evaluations", Fabian et. el. 2010, p. 7. Fabian et. al. criticize the Common Criteria for assuming the stakeholders in a system are the same as its owners. According to Fabian et. al., this assumption is false, as it does not provide for the often occurring reality that stakeholders in a system are different from the system owner. Security requirements engineering, especially the multilateral variant, explicitly assume that the interests of the many possible stakeholders in a system can conflict. These dynamics are particularly relevant for policymaking, and have informed the choice to cover (multilateral) security requirements engineering in detail in this section.
increases from the attributes of the c.i.a.-triad, to security goals, to requirements, and finally to specifications that systems engineers use to build secure systems.\textsuperscript{446}

Security requirements in engineering are defined by Haley et al. as ‘constraints on the functions of the system, where these constraints operationalize one or more security goals.’\textsuperscript{447} Fabian et al distinguish three aspects of security requirements: i) they capture security goals in more detail; ii) they indicate a stakeholder and a counter-stakeholder; iii) they describe the applicable laws or other circumstances in which they operate.\textsuperscript{448} Security requirements can originate from the security goals of the developer of a system, as well as from the ‘outside world’, for instance contractual agreements with clients or legal obligations in regulation. Again, law is recognized as playing a vital role in determining security requirements, as observed in the previous sections.

Security Quality Requirements Engineering (SQUARE) is one of the prominent methods in this field of computer science. SQUARE is a nine-step process developed at the Software Engineering Institute of Carnegie Mellon University.\textsuperscript{449} It helps organizations to build security into the early stages of the production life cycle.\textsuperscript{450} Both security engineers and stakeholders participate in the nine-step process, which is designed as follows:\textsuperscript{451}

1. Agree on definitions.
2. Identify assets and security goals.
3. Develop artefacts to support security requirements definition.

\textsuperscript{446} Fabian et al 2010, p. 12.
\textsuperscript{447} Haley et al 2006, p. 37. Fabian et al conclude that “there is no established terminology in the field of security requirements engineering”, Fabian et al 2010, p. 38.
\textsuperscript{449} Fabian et al. 2010 compare SQAURE with different other methods.
\textsuperscript{450} See <https://www.cert.org/sse/square/>, accessed 2 September 2015.
\textsuperscript{451} See <https://www.cert.org/sse/square/square-ninesteps.html>, accessed 2 September 2015.
5. Select elicitation technique(s).
6. Elicit security requirements.
7. Categorize requirements.
8. Prioritize requirements.
9. Inspect requirements.

Each of these steps has a range of inputs, techniques, specific participants and outputs, described in detail in SQAURE documentation.\(^452\) The first step is to agree on definitions, because different stakeholders have different ideas on what general concepts mean. The second step is considered vital in the SQAURE process: “without overall security goals for the project, it is impossible to identify the priority and relevance of any security requirements that are generated.”\(^453\) Towards the end of the process, security requirements are identified, categorized, prioritized and inspected (step 6-9). It should be noted that SQAURE generates as specific requirements as possible: ‘the call center website mode should be available to at least 300 connections at any given time’ is an example of such a requirement, where ‘the system shall improve the availability of the existing customer service center’ is a security goal. SQAURE intends to result in a set of prioritized goals and requirements which inform the design of the system.

**Multilateral Security**

The concept of multilateral security further addresses conflicting interests of different stakeholders in the same system. Multilateral security is defined as:\(^454\)

\(^{452}\) A tool that guides the participants of the SQUARE through the process can be downloaded from the project website. See <https://www.cert.org/sse/square/square-tool.html>, accessed 2 September 2015.

\(^{453}\) See <https://www.cert.org/sse/square/square-faq.html>, accessed 2 September 2015.

\(^{454}\) Pfitzmann 2006.
“providing security for all parties concerned, requiring each party to only minimally trust in the honesty of others:

- Each party has its particular protection goals;
- Each party can formulate its protection goals;
- Security conflicts are recognized and compromises negotiated;
- Each party can enforce its protection goals within the agreed compromise.”

Rather than neglecting conflicting interests of various stakeholders that take part in a system, multilateral security “supports engineers in identifying security goals of the security stakeholders, and in resolving conflicts among them.”\(^{455}\) As such, it has “the potential to free users of IT systems from a lack of self-determination concerning their (in)security.”\(^{456}\)

Several methods for eliciting these requirements from multilateral security analysis have been described by Fabian et al. and have been operationalized by a range of authors, such as Gürses & Santen.\(^{457}\) Upon finishing a security engineering process, such as SQUARE, these authors argue that a multilateral security engineering analysis must be conducted to illuminate and consolidate stakeholder interactions and conflicts. Fabian et al. describe one influential method, the Multilateral Security Requirements Analysis (MSRA):

1. Identify stakeholders.
2. Identify episodes.
3. Elaborate security goals.
4. Identify facts and assumptions.
5. Refine stakeholder views on episodes.
6. Reconcile security goals.
7. Reconcile security and functional requirements.

\(^{455}\) Fabian et al 2010, p. 8.
\(^{456}\) Pfitzmann 2006.
\(^{457}\) Gürses & Santen 2006 conducts a case study of multilateral security requirements for an Intranet environment for Ph.D. students.
As with the SQUARE model, the security goals in MSRA are derived from the c.i.a.-triad. A particularly valuable insight for legislating communications security in the multilateral approach is that stakeholders not only have conflicting interests in terms of the security goals (some might prioritize confidentiality, others availability) relating to themselves in isolation, but also that stakeholders might have similar interests that conflict in relation to another stakeholder. Multilateral security engineering therefore ties a counter-stakeholder to a stakeholder with an interest in a particular security requirement. For example, a user may have a confidentiality interest in a social network towards the social network, an attacker, other users and/or the government. Crucially, in multilateral security engineering different goals from different stakeholders is not seen as problematic, but as essential informative input to any security policy. It provides necessary insights to elaborate, negotiate, balance and enforce the conflicting stakeholder interests. In the process, multilateral security “requires each party to only minimally trust in the honesty of others,” as the process is meant to illuminate these conflicts.

Clearly, security requirements engineering is a different affair than drafting legislation. In policymaking and regulation, there is no such thing as a systems engineer who has control over a designing process in a similar way. But just as positive and negative stakeholder interests are “necessary and fruitful” for a requirements engineering team, legislatures should engage with these methods to illuminate such underlying values and interests when legislating communications security. The interaction of stakeholder interests is an essential insight into determining how to balance the security attributes in a specific communications function. Employing such insights would for instance suggest explicitly and openly mediating conflicting stakeholder interests with regard to

458 Fabian et al. 2010, p.16-18.
459 Pfitzmann 2006.
460 Fabian et al 2010, p. 12.
confidentiality, integrity and availability in legislative debates on private communications security at the EU level.

Both SQUARE and MSRA take the c.i.a.-triad as their central conceptual framework and show that it can be applied to all forms of systems, or communications functions. Both methods necessitate a transparent statement on the expected security goals of a process and the identification of threats to those goals, or external requirements such as legal obligations. Subsequently, both methods expect conflicting interests of stakeholders in the process, as in any legislative process. MSRA in particular explicitly obliges these conflicting interests to be resolved in an open, transparent negotiation between affected stakeholders as part of the design process – one can imagine how tools such as hearings and consultations may contribute in similar ways in legislative processes. Security goals are then prioritized; some goals must be met, others may be considered less critical. Assurance approximations are then made of the expected outcomes, which leads to another iteration in the design process. Finally, design or legislative interventions can be devised and its outcomes inspected – a role in the legislative process for institutionalized enforcement. In all these stages, the generalized procedural model requires specification based on the system at hand. These models could inform a general model for legislating communications security, tailored to the specific circumstances of the communications function under scrutiny. These insights will be used to inform the conceptual framework and regulatory model for the case studies in Part III, as proposed in chapter 7.

Finally, one important but often overlooked point is the impact of different understandings of the elements of the c.i.a.-triad both between regulators in different jurisdictions and between technical and policy communities. The contentious issue of the legal protection of communications ‘metadata’, discussed in chapter 4, may illustrate the importance of explicit normative
guidance on the security attributes of the c.i.a.-triad. Whereas both content and metadata are afforded fundamental rights protection within the meaning of confidential communications under article 8 ECHR and EU legislation, metadata seems to enjoy little, if any, comprehensive constitutional protection in the US. The EU lawmaker must realize that these different understandings can have real consequences, for example when delegating details of legislative provisions to technical standards negotiated in international organizations or self-regulatory industry associations. International technical forums such as the IETF or the IAB lean heavily on US expertise and legal perspectives. These standards have a large impact on actual communications security enjoyed by EU citizens and are often referred to in EU legislation. Yet another argument why explicit and specific normative guidance on the part of the EU lawmaker is vital when the c.i.a.-triad is employed as a conceptual framework for EU lawmaking on private communications security.

5.4. Failure Classes: Surveillance, Users, Technology, Markets

When communications security fails, the root cause of failure can often be traced back to underappreciated threats and vulnerabilities. Threats that may affect a system adversely are called a vulnerability. When a vulnerability materializes, security fails. Security failure is frequently related to early phases of a systems design process. In many security requirements engineering

461 See section 4.2.
462 See for example Smith v. Maryland 442 US 735 (1979), which ruled that telephone metadata is not a “search” under the 4th Amendment of the US constitution. United States v. Fregoso, 60 F.3d 1314, 1321 (8th Cir. 1995) held that stored telephone records are not protected either. In United States v. Perrine, 518 F.3d 1196, 1204 of 2008, the 10th Circuit held that “Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation”. The 9th Circuit held the same with regard to IP-addresses in United States v. Forrester, 512 F.3d 500, 510. The observation might change in the near future, as court cases launched in the wake of Edward Snowden’s disclosures go upstream in the US court system. The
463 See chapter 2.
464 Pfleeger 2003, p. 504.
methods, such as SQUARE described above as well as threat modeling and composition, a risk analysis is conducted to illuminate possible security threats and vulnerabilities. When threats have been appropriately modeled, systems design can take these into account in the earliest phases of systems engineering. The concept of ‘privacy by design’ – engineering privacy into systems – is enjoying evermore traction in EU law, most notably the data protection cycle (see section 2.2). But for the EU lawmaker itself, it helps to similarly anticipate threats and vulnerabilities in law- and policymaking.

As such, it is crucial to have a broad understanding of the failure classes of communications security. Confidentiality, integrity and availability vulnerabilities and threats can have various causes. This study will not comprehensively describe all of them or provide an exhaustive taxonomy, but outline four important causes for security failure. These are i) surveillance; ii) user; iii) technology, and iv) market failure. The four classes are not mutually exclusive or collectively exhaustive, and may overlap with one another as the following simple citation shows:

Website operators are reluctant to switch to more secure protocols if this will lose them even a few percent of prospective customers who are still using old software, so vulnerabilities introduced deliberately during the Crypto Wars have persisted to this day.

The four classes all emerge in the citation. They help to quickly grasp the underlying dynamics behind communications security failures. A brief overview is given in this section.

465 Another way to illuminate such threats is through threat modeling, or exposition. For an example in BGP, RPKI and DNS communications, see: Arnbak & Goldberg 2015.
466 See Anderson 2011.
467 Abelson et. al. 2015, p. 16.
Surveillance is an increasingly important cause. Several Snowden disclosures showed persistent efforts by intelligence agencies to manipulate and subvert widely used Internet protocols (BULLRUN) and routers (TURBINE). Part I discussed the GSM case and the crypto wars of the 1990s. Built-in vulnerabilities in communications infrastructure for wiretapping purposes is not merely an issue of the past, but very much a topic of debate in 2015, as we purportedly are living through the “crypto wars 2.0”. Such covertly or explicitly mandated backdoors are incompatible with design practices that seek to minimize the implications of data and communications breaches after occurrence, such as “forward secrecy”. Surveillance backdoors also introduce more complexity into communications software and infrastructure, which is likely to have major unintended consequences for communications confidentiality, integrity and availability. Legislation can play an important role in both enabling and limiting such communications failures, and chapter 4 discussed surveillance as a failure class from a constitutional and normative perspective. Chapter 9 conducts a case study into ‘cloud’ communications and surveillance as a cause of communications security failure.

Second, security may fail because of user behavior. Weak passwords and not regularly updating software belong to two concerns in a long list of user behavior contributing to security failure. Apart from basic user conduct, such as choosing robust passwords, securing communications is impossible for average and even tech-savvy users. Usability of computing and particularly communications security technologies is extremely difficult for the average user. Providers and developers maintain a long tradition of placing onerous obligations on users, as well as letting users bear the full cost of failure of

---

468 Abelson et. al. 2015.
469 Abelson et. al. 2015.
470 See for instance the Internet Toolbox of NGO Bits of Freedom, available at <https://toolbox.bof.nl/>, for a list of security concerns and what the average user can do to protect communications.
471 Whitten & Tygar 1999.
communications security. The practice is known as ‘liability dumping’, explained in section 5.5 and is both observed and discussed in the HTTPS and ‘cloud’ communications case studies of Part III.

Technology itself inherently comes with flaws, even if security requirements engineering is aimed at minimizing technological vulnerabilities. Systems are increasingly complex and interdependent, as technology develops.\footnote{Schneider 1999.} At the turn of the millennium, Windows 2000 already contained around 35 million lines of code, leading Anderson to estimate around 1 million bugs in the most widely used operating system of the day.\footnote{Anderson 2001.} Windows 7 contains 40 million lines of code, Google’s Chrome Browser about 5 million, and Android OS upward of 10 million lines.\footnote{See for example <http://www.informationisbeautiful.net/visualizations/million-lines-of-code/>, accessed 2 September 2015.} The amount of exploitable bugs in these systems is quite huge. In addition, networked communications technologies depend on other systems. In his infamous 1984 ACM Turing Award acceptance speech on “Reflection on Trusting Trust”, Ken Thompson illustrated that “you can’t trust code that you did not totally create yourself.”\footnote{Thompson 1984.} Against this background, it is not surprising that leading computer scientists write that “from a scientific perspective, there is no absolute notion of security.”\footnote{Boneh & Mitchell 2012, p. 1660.} With abounding complexity and interdependence, a certain tolerance for complexity failure in soft-, hardware and protocols seems desirable.\footnote{Appreciating technological complexity seems also recognized by the ECtHR, in its short inadmissibility ruling \textit{Muscio v. Italy} concerning spam. As the ruling concerns a very specific case and set of facts, was declared inadmissible, and presided over only by a single judge, it is not clear whether the ruling itself will have a huge impact in future rulings. ECtHR, Muscio v. Italy, No. 31358/03, 13 November 2007.} Security is hard, and it takes time and investment to provide acceptable secure communications to end users.
A fourth failure class is connected to these observations on technology. Increasingly well-understood are classic *market failures* in communications security. The relatively new and influential academic discipline of security economics studies market failures in technical security engineering. Security economics is described in the next section.

5.5. **Security Economics**

The burgeoning field of research into security economics can be considered a subfield of highly influential work of standard economic theory applied to Internet markets, which has won a Nobel Prize\(^{478}\) and is otherwise widely referenced in the latest information security research.\(^{479}\) Security economics posits that systems security fails when organizations or users that defend the systems lack an economic incentive to do so. Or in the words of Moore and Anderson:\(^{480}\)

> “Systems often fail because the organizations that defend them do not bear the full costs of failure. This simple insight has profound consequences for a growing number of industries, and it extends to dependability as well as security.”

Through its incentive-based analysis, security economics has explained various persistent security failures throughout the electronic communications environment using classic economic theories, such as information asymmetries, externalities and liability dumping. Three classes of regulatory intervention have emerged in security economics theory to help combat perverse market

---

\(^{478}\) The 2014 Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel was awarded to Jean Tirole in honor of “his analysis of market power and regulation”, see <http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2014/tirole-facts.html>, accessed 2 September 2015. For instance, see Rochet & Tirole 2003.

\(^{479}\) Shapiro & Varian 1998.

\(^{480}\) Moore & Anderson 2011.
incentives: security requirements (‘technical and organizational measures’), transparency obligations (such as security breach notifications) and liability arrangements. These measures and their appropriateness are extensively discussed in the case studies of Part III.

Security economics has found market failures and explained security breaches in leading security industries such as online banking, operating systems development and electronic health care. Indeed, frequently it emerges post-breach that organizations failed to adopt fairly straightforward security policies and measures. In the infamous DigiNotar breach that paralyzed HTTPS communications, for example, the Certificate Authority kept quiet about a deep security breach across their systems and networks for over three months. Years later, during court proceedings, it became clear that the Certificate Authority failed to adopt as many as 30 critical software patches; a practice an external IT consultant had warned against three consecutive years before the breach. Security economics can be an important tool for examining source for illuminating such security failures. Moreover, it fits well into the theory behind multilateral security requirements engineering, as it acknowledges and analyzes different interests of various stakeholders that operate within a communications setting.

Chapter 4 argued that, after CJEU Digital Rights Ireland, economic considerations of market players and a hands-off approach of the EU lawmaker fail to sufficiently protect the enjoyment of fundamental rights by end users in the networked environment. Security economics can be helpful in illuminating where markets fail to produce communications security up to the level of

481 Critiqued by the CJEU Digital Rights Ireland decision annulling the Data Retention Directive, as discussed in section 4.2.
482 See Anderson et. al. 2008. These measures are studied in chapter 8.
483 Moore & Anderson 2011.
484 See section 8.2.
safeguards required by the EU Charter since *CJEU Digital Rights Ireland*. In 2008, Anderson et al. published a comprehensive study commissioned by ENISA with broad recommendations for the EU lawmaker to address market failures in security provisioning across the networked communications environment. Meanwhile, Part I of the study showed how some measures of the security economics toolkit as proposed by Anderson et al. have been adopted across EU policy cycles, although in a haphazard, incoherent and often ultimately weakened form. To delve deeper into the role of the EU lawmaker and the usefulness of security economics as a method for illuminating market dynamics vis-à-vis fundamental rights obligations, chapter 8 will deploy security economics methods in a case study on HTTPS communications.

### 5.6. Conclusion

The chapter concludes that the c.i.a.-triad can provide the basis of the conceptual framework to legislate communications security through EU law. But stating its elements at the start of a legislative instrument does not provide sufficient specificity. In the definition of the c.i.a.-triad, authorization is a central concept that must be further developed. Security requirements engineering methods can be employed to provide the specification and balance between confidentiality, integrity and availability interest in the communications uses that are regulated under a particular EU legislative instrument. In addition to substantive guidance by fundamental rights law, the concepts and tools of systems design should provide procedural concepts and tools to guide EU communications security legislation. Security economics scholarship provides the EU lawmaker with a concrete legislative toolkit.

---

485 Anderson et. al. 2008.
486 See chapter 2 and in particular section 2.7.
In conclusion, the c.i.a.-triad and the centrality of authorization mandate procedures to negotiate the underlying interests of security, while providing substantive flexibility to do so according to the specific communications functions and use cases at hand. The step by step models of security requirements engineering provide inspiration on how to map a comprehensive stakeholder environment and the systemic vulnerabilities that put pressure on a certain communications use case. Fundamental rights and data-driven insights from security economics must fill the void of the conceptual ambiguity around legislating communications security found in part I. From a fundamental rights and systems design perspective, robust legal requirements for end-to-end-security seem appropriate to address pervasive surveillance failures. Conceptually, end-to-end communications security could serve as a practical extension of the legal concept of communications secrecy in letters and telecommunications. These observation provide critical input for the design of the case studies of Part III.
6. Political Perspectives

The previous chapters have developed a functional conceptualization of communications security, based on the c.i.a.-triad, security requirements engineering and infused with constitutional analysis. But the historical analysis of Part I has made clear that there can be canyons between theoretically robust conceptualizations and how legislation takes shape in the political arena. Doctrines of deterrence and protection compete with one another, along with national security vis-à-vis technical security, in current conceptualizations of ‘security’ in EU communications law and policy.

One central question this chapter explores, is: “why ‘security’?” As a concept, ‘security’ is notoriously vague, ambiguous and multi-layered. Even if a wealth of related concepts exist in the technical literature – ‘robustness’, ‘resilience’, ‘dependability’ – the ‘security’ frame has been dominant in EU policy debates since the 1990s. This chapter examines the framing of protecting private communications in terms of ‘security’, and illustrates that the ‘security’ frame has profound policy consequences. The chapter does not offer an exhaustive taxonomy or political definition of ‘security’. Instead, several theories from political science are surveyed to gain a deeper insight into the political realities of framing the protection of private communications as ‘security’ – particularly, as ‘cybersecurity’ – at the EU level. The EU lawmaker needs to understand and confront these powerful political dynamics – including subjective security, ‘securitization’ and the implicit politics in technology policymaking – that both intentionally and unintentionally lead to a circumvention of transparent legislative debates to secure political and economic agendas. As such, the framing of protecting private communications as a matter of ‘security’ has profound implications for the viability of protecting private communications for end users through EU law.

General security discourses, practices and political science literature are surveyed. After describing the ambiguity of the political conception of security in section 6.1, section 6.2 outlines the modalities of political ‘security’. Then, the influential political discursive practice of ‘securitization’ will be introduced to describe and elaborate on the emphasis of security vis-à-vis other concepts. Finally, these general theories on the political conception of security will be held against the historical analysis of Part I of this study, to highlight the importance of framing in the legislative capacity of the EU in the area of communications security.

6.1. The Political Conception of ‘Security’

Contrary to many concepts in law and politics, ‘security’ immediately rings a bell with non-lawyers. ‘Security’ evokes primary emotions and instincts of survival, present in animal and human cognition, central to survival and maintaining your species. Moreover, security is perceived entirely differently from one person, culture or civilization to another. Some define security as being safe from harm. Others see it as not being exposed to any risk or threat. In technical communities, security is often seen as the means to achieve freedom from corporate or state surveillance. All use the ‘security’ frame but appeal to entirely different underlying values. To make matters even more complex, language and local culture play a significant role in how ‘security’ is conceptualized. In Chinese policy circles, for example, censorship of online speech is framed as “information security” policy. Therefore, Zedner calls the political concept of security ‘slippery’:

“Its meanings are multiple and without clarity about which meaning is intended (or understood); exactly what is being provided and consumed, sold and bought, promised or sought remains obscure.”

Ambiguity abounds around the concept of ‘security’, as its exact meaning remains obscure. Zedner argues that imprecision can be both unintentional and intentional, and may give rise to ‘divergent’ and ‘exceptional measures that might be otherwise indefensible’.491

Between theory and practice, facts and emotions, objectivity and subjectivity, a wide range of interests underlie the political conception of ‘security’. Some herald security as the ‘hallmark of civilizations’.492 Others use terms as ‘security theatre’ to point at our obsession with the concept,493 or observe that ‘security has […] become inextricably entwined with the circuits of accumulation in contemporary capitalism’.494 The following sections shed some light on these interests.

6.2. Security Modalities: Material and Procedural

Security exists in several modes: both as a state of being or what one might call ‘material security’ and as a means to an end or ‘procedural security’.495 The former captures its substantial manifestation, while the latter covers the process of security production. This section introduces these concepts, and situates them in a broader analysis of contemporary changes in human organization.

Material Security: Objective and Subjective

491 Zedner 2003, p. 158.
493 Schneier 2003, p. 38
494 Yar 2009, p. 190.
495 Zedner 2003.
Material security, security as a state of being, can be separated into *objective* and *subjective* security. Zedner describes three conditions of objective security: i) absolute security without threats; ii) a neutralization of threats, ‘being protected from’, and iii) non-exposure to threats.\(^{496}\) The first form is a hypothetical situation. Absolute security does not exist in the real world, not even in a police state, as the popular saying goes. So-called “ontological insecurity” has always been a fact of life. For information, communications or computer security, reality is nothing different.\(^{497}\) Zedner’s second and third form are most commonly deployed. But neutralization and non-exposure create a connection between objective security and the threats to it: security cannot exist without threats. Fundamentally, objective security needs threats to sustain it as a concept.

Material ‘subjective security’ describes feelings, rather than objective facts. It exists both in a positive and negative form. Positively framed, it can be described as feeling safe. Negative subjective security refers to insecurity, a state of fear or anxiety. The growing mismatch between objective and subjective security and a rising emphasis on subjective security has been observed by many. At the same time, fear and anxiety, for instance regarding terrorism and crime, abound. There is hardly a logical explanation for this. Pinker reflects on the 9/11 attacks that killed nearly 3,000 people. Meanwhile, “[e]very year more than 40,000 Americans are killed in traffic accidents, 20,000 in falls, 18,000 in homicides, 3,000 by drowning (including 300 in bathtubs), 3,000 in fires, 24,000 from accidental poisoning, 2,500 from complications of surgery, 300 from suffocation in bed, 300 from inhalation of gastric contents, and 17,000 by “other and unspecified nontransport accidents

---

\(^{496}\) Zedner 2003, p. 155.  
\(^{497}\) Zalewski 2011; Anderson 2008. See section 5.4 on technology as a failure class.
and their sequelae.” As Pinker puts it, “Western Europe at the turn of the 21st century [is] the safest place in human history”.

Comprehensive analysis of the mismatch between objective and subjective security, and the growing influence of the latter in politics, needs to speak to a broad set of fundamental shifts in human organization over the last decades. Yar identifies two separate lines of inquiry into these social transformations, one ‘epochal’ and the other more specific on the manifestation of ‘capitalism’. The epochal line of inquiry is further explored below. The intimate connection between the political conception of subject security and capitalism will be more comprehensively discussed in section 6.3 on ‘cyber’ securitization.

Already in the 1990s, Giddens observed that (Western) ‘societies are increasingly pre-occupied with the future (and also with insecurity), which generates the notion of risk’. And Beck famously coined the concept of the ‘risk society’, describing it as ‘a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself’. Modernity, urbanization and globalization all belong to such common ‘epochal’ generalizations that may broaden the view of this study so far to provide, not the explanation, but a window into our complex contemporary condition.

---

498 Pinker 2011, p. 415.
499 Pinker 2011, p. 62. See also p. 415.
500 The analysis here is far from exhaustive, but highlights several developments often found in security literature in the social sciences. It serves to illustrate the main point that while necessary for regulatory purposes, the conceptualizing ‘security’ is never complete and must be situated in a broader analytical understanding of what underlying values and discursive and political practices are at hand when we refer to the concept of ‘security’.
502 Giddens 1999, p. 3.
The maturing of information age with its always increasing global connectivity exacerbates the complexity.\textsuperscript{504} With Foucault, Aas et al. observe how ICTs are have become a central instrument of governance today:\textsuperscript{505}

\begin{quote}
\textit{The ability of ICTs to not only watch and record but communicate and articulate is transforming the nature of our knowledge and sociality. Technologies are an essential aspect of modernity, and through the progressive convergence of production, communication, knowledge and surveillant technologies (...) they are ingrained in some of the central tasks of contemporary governance.}
\end{quote}

De Mul et al. argue that our condition, particularly exacerbated by how ICTs are more and more intertwined in daily life, is already moving beyond modernity theory. In this view, transition into (post-)modernism makes our condition even more paradoxical, unpredictable and uncontrollable\textsuperscript{506}– which may be the case in policymaking around global warming, financial crises, education, immigration or the rise of the national surveillance state. Even though the debate on whether to frame the contemporary human condition as modernity or (post-)modernity is very much open, the underlying observation is quite uniform: complexity abounds.

Every layer of society, from government to the individual, is finding ways to deal with complexity and major shifts in social, economic and political organization. Bauman speaks to both the policy and personal perspective when he observes a ‘transfer of anxiety’: \textsuperscript{507}

\begin{quote}
\textit{In an ever more insecure and uncertain world the withdrawal into the safe haven of territoriality is an intense temptation. It is perhaps a happy coincidence for political operators and hopefuls that the genuine problems of insecurity and uncertainty have condensed into}
\end{quote}

\textsuperscript{504} Castells 2009.
\textsuperscript{505} Aas, Gundhus & Lomell 2009, p. 6.
\textsuperscript{506} De Mul, Müller & Nusselder 2001, p. 106-108.
\textsuperscript{507} Bauman 1998, p. 116-117.
Bauman’s main point is, quite literally, a bit lost in translation. In the same work, Bauman explains that in German, the word ‘Sicherheit’ captures the words ‘certainty’ and ‘safety’ in addition to ‘security’ and directly appeals to the quite recent East-West divide. But Bauman’s essential insight is that re-framing uncontrollable major shifts in human organization as ‘security’ threats creates the appearance of control and agency. Put differently, global social, economic and political shifts are re-claimed by national and local agents as security issues to create the appearance that something can be done about it. Moreover, the state and industry, Bauman argues, have direct interest in these social dynamics: “A lot of tension accumulates around the quest for safety. And where there is tension, political capital will surely be spotted by bright investors and expedient stockbrokers.” The ‘security’ frame is also dominant in contemporary politics: the re-branding of the Dutch ‘Ministry of Justice’ into the Ministry of ‘Security and Justice’ (signaling to the public that security trumps justice) in 2010 is a case in point. As such, a lot of political and economic capital seems to be on the line in ‘security’ policymaking.

The described transfer of anxiety and creation of an appearance of control through the ‘security’ frame may provide a deeper explanation for the mismatch between objective and subjective security. The extent to which such ‘epochal’ theories of security can be measured remains limited, but in the literature a consensus seems to exist that the political incentives for

---

508 Bauman 1998, p. 117. This adds an important additional perspective to discursive analysis of ‘security’, such as securitization (discussed below): the relevance of local language and culture. Given the linguistic and cultural properties of ‘Sicherheit’, Bauman warns for a greater potential for political exploitation in the German language. It goes beyond the scope of this research to exhaustively flesh out such linguistic nuances.


510 Translated from ‘Ministerie van Veiligheid en Justitie’. Decided by Royal Decree, K.B. van 14 oktober 2010, kenmerk 3096356. H.
emphasizing ‘security’ are real. These ‘epochal’ theories around security also feed into the second modality of ‘security’.

Procedural Security

‘Procedural security’, or security as a means to an end, refers to the process in which the pursuit of security becomes an end in itself. Procedural security also thrives on the existence of threats, but does not necessarily produce objective, or even subjective security. According to Aas et. al., procedural security often has a detrimental effect on its material counterpart:511 ordinary arenas such as the city center, the workplace or the Internet, as well as ‘mundane objects (such as scissors and water bottles) and activities are becoming bearers of risks which need to be neutralized’.512 When the outcome of a policy becomes less relevant, so do facts and evidence. Even more than material security, procedural security is a continuum, a never-ending pursuit.513 As such, it is a particularly useful tool to secure funding or political agendas.

The rise of subjective security at the cost of objective security, or Bauman’s transfer of deeper anxiety into ‘security’ threats, intensify the procedural manifestations of security politics. Both governments and voters seem comfortable with the security surge in recent years. The former Dutch Minister of the re-branded Ministry of Security and Justice Ivo Opstelten continuously acknowledges that subjective security concerns are driving his policy agenda, rather than objective security levels. He is supported in his statements by politicians, influential think tanks, industry and voters across the political

511 Yar 2009, p. 189. Specifically, This occurs, for instance, when a false sense of secure communications lets involved parties disclose more sensitive information. With the DigiNotar breach, the Gmail communications of reportedly 300,000 Iranians were compromised, which according to some commentators may have led to subsequent arrests.
512 Aas, Gundhus & Lomell 2009, p.2.
513 Zedner 2003, p. 156.
spectrum.\textsuperscript{514} The surge cannot be empirically linked to a rise or fall of terrorist threats, crime rates and so forth.\textsuperscript{515} In addition, the gap between subjective security and objective facts seems to be widening on the individual level.\textsuperscript{516} Taylor argues that this re-framing of general anxieties into subjective insecurity may have to do with the fact that security concerns have become a socially acceptable avenue for resentment.\textsuperscript{517}

The described mismatch between objective and security contains a vital insight for legislating communications security. Not only may independently established facts be quite irrelevant in security policymaking. More fundamentally, political security theorists seem to agree that contemporary society and citizens at large may not necessarily be seeking objective security in the first place. The process of security production has arguably become of greater political importance, than materially augmenting security. Rothschild identifies as the ‘crudest purpose’ of security policy the desire ‘to influence directly the distribution of money and power.’\textsuperscript{518} In such views, a lot more is at stake in EU security policymaking than assuring secure communications. Nissenbaum & Nissenbaum, for instance, argue in 2009 that cybersecurity policy has successfully been ‘securitized’.\textsuperscript{519}

\textsuperscript{515} Zender 2003.
\textsuperscript{516} Fact is, for instance, that amidst the growing security emphasis, actual crime rates have been falling spectacularly since the 1990s across the Western world. See Pinker 2011. See also <http://www.economist.com/news/briefing/21582041-rich-world-seeing-less-and-less-crime-even-face-high-unemployment-and-economic>, accessed 2 September 2015.
\textsuperscript{517} See for instance Taylor 1998, p. 23.
\textsuperscript{519} Hansen & Nissenbaum 2009, p. 1160.
6.3. ‘Cyber’ Securitization

In addition to ‘epochal’ theories around the emphasis of the rise of subjective and procedural security, one can also study the discursive practices in security politics. In 1998, the Copenhagen School introduced the now influential analytical tool of “securitization”. Rooted in international relations and international security theory, securitization scholars argue that to understand the political incentives behind the contemporary emphasis on ‘security’ in policymaking, one needs to focus on ‘speech acts’ that seek to achieve political effect – for instance, achieving priority and funding for particular political agendas.

The Copenhagen School separates three stages of public policy discourse: i) nonpolitical (no state action); ii) political (public policymaking), and iii) securitized. Three essential elements determine successful securitization: issues must be framed as i) imminent and existential threats, ii) to a significant collective and iii) by a potent actor who is accepted by surrounding communities. Successful securitization frames a public policy issue as an emergency in which legal and social rules may be suppressed, instead of public policy as usual. The latter insight is essential in understanding the political force of the ‘security’ concept. For instance, securitization takes away the need for empirical evidence to support the claimed potential of proposed security technologies and measures. In such circumstances, anecdotal or incomplete support material suffices and real evidence may be taken for granted. In other words, after successful securitization “security is what a political actor or a

521 Buzan et al. 1998, p. 23. See also Nissenbaum 2005, p.25. See also Hansen & Nissenbaum 2009, p. 1159. The latter argue that all public policy issues are essentially political, but that media and political attention play a decisive role in whether a public policy issue becomes politicized.
522 Aas, Gundhus & Lomell 2009, p. 3.
political entity labels as security in a particular situation”. Interestingly, these are all developments well-known and well-covered before ‘9/11’, but the subsequent ‘war on terror’ has exacerbated practices of securitization.

In securitization theory, the state counts as the primary recipient and producer of securitization. Walker interestingly observes in 1990, that precisely because of long developed and well-known institutional state mechanisms, the state and in particular its concept of national security are well-positioned for resolution of conflicting claims to identity, order and authority. Beyond terrorism and law enforcement policy, the economy, the environment, air travel and religion have been identified as securitization sectors. In addition, Hansen & Nissenbaum now argue that ‘cyber-security is successfully securitized’ in US policymaking. Deibert & Rohozinski have repeatedly done so since 2003, adding to a long line of research about the militarization of cyberspace. In 2013, Deibert argued that “as the securing of cyberspace unfolds, ensuring basic principles of transparency, accountability and mutual restraint will be critical. (..) There is an urgent need for the articulation of an alternative cyber-security strategy for civic networks and from the perspective of liberal democracy”.

---

524 Nissenbaum 2005.
527 Deibert & Rohozinski 2008. See also Deibert 2003. A very different perspective comes from international security studies that adopt traditional conceptions of political security, and argue that global distributed networked communications entail ‘international anarchy’ for the state. For instance Kello 2013, p. 39.
528 Deibert 2013.
At the same time, Zuboff observes that surveillance capitalism now rules the ‘information civilization’.\textsuperscript{529} Government and corporate interests thrive, and are “mutually reinforcing”,\textsuperscript{530} in the mode of existence of capitalism in which pervasive surveillance has become practice. Already described as ‘the invisible handshake’ by Birnhack and Elkin-Koren in 2003,\textsuperscript{531} or the ‘surveillant assemblage’ by Haggerty and Ericson in 2000,\textsuperscript{532} it has become evident that availability of data in the private sector and accessibility for government purposes are interdependent: without such data storage and processing practices in the private sector, the intrusion into the private sphere by public authorities through data gathering would be restricted – and perhaps confined to more targeted operations. Today, abundant communications and data has made surveillance more valuable and lowers transactions costs for access as, in particular, cloud providers become a one-stop shop for data.

As the literature appears not to have established a full-on securitization of EU communications security law, these ‘epochal’ analyses matter for the EU lawmaker. Even if some of these theories are US centric, they are relevant to the EU lawmaker as communications infrastructures and services are to a considerable extent shaped in the US.\textsuperscript{533} Moreover, the Snowden disclosures have implicated Western intelligence agencies and companies on both sides of the Atlantic. The findings of Part I seem to suggest that the securitization dynamic is at play. For decades, policies focus on deterrence rather than protection as a security strategy. The explicit, implicit and covert national security capture of EU policymaking by national security interests is another key development observed in Part I.\textsuperscript{534} In addition, the surveillance industry is promoted by the European Commission as a growth sector in Europe and a key

\textsuperscript{529} Zuboff 2015, p. 75–89.
\textsuperscript{530} Aas, Gundhus & Lomell 2009, p. 7.
\textsuperscript{531} Birnhack & Elkin-Koren 2003.
\textsuperscript{532} Haggerty & Ericson 2000. See also Schneier 2013.
\textsuperscript{534} See sections 3.3. and 3.4.
funding opportunity on its research programs. Technical security and privacy do not enjoy such prioritization.

Political and economic interests thus seem to favor securitization, rather than balanced policies to protect private communications security through EU law. However, to establish the extent to which securitization claims can be made with regard to EU communications security law lies beyond the scope of this study. The EU lawmaker should, nonetheless, be fully aware of such deeper political dynamics that obstruct objective security goals in favor of subjective security measures to serve political and economic ends, rather than technical assurances for private communications security.

6.4. Implicit Politics of Technical Policymaking

In addition to the more explicit political framing of security, discussed in previous sections, the framing of a security politics as a highly technical issue often indicates implicit politics, particularly, when a policymaker allows technical experts to monopolize a policy space and its discourse.

Technology is a complex policy area. Part I of this study established that the EU lawmaker often delegates the details of communications security policy to lower legislation, standards or self-regulation. In addition, non-technical policymakers often regard the technical aspects of a policy matter as a given, or


536 In addition, state and corporate interests in weak communications security protection often run parallel to one another, exacerbating the power of securitization. Public-private security and surveillance partnerships have been around for centuries in the communications environment, and have been particularly sprawling recently. See Marsden 2014.
a ‘black box’\textsuperscript{537} that for some input renders an output that cannot be influenced nor discussed. The difficult, but necessary political debate on the technical details of, say, a communications protocol\textsuperscript{538} does not occur, while the ‘awe’, promises or perils presented by technologists are incorporated in policy with little or no debate. Meijers discusses the fact that most Internet users do not understand the “invisible protocols of the Internet”, and argues that through the use of information technology the anatomy of decisions is obscured with the result that certain governmental acts are less open to contention.\textsuperscript{539}

This complexity can obscure the politics that are often embedded in technology policy.\textsuperscript{540} A subfield of sociology – ‘technosociology’ – studies these deeper politics implicitly embedded in technology, for example in the standardization of mobile communications protocols.\textsuperscript{541} Nellis has coined the term ‘techno-managerialism’ \textsuperscript{542} to describe the general trend that technologists prioritize goals such as efficiency, effectiveness and modernization, rather than democratic values and resolving deeper social problems through non-technical, more humanistic approaches.\textsuperscript{543} For instance, in the realm of law enforcement, surveillance technologies often replace conventional, non-technical and more relational modes of supervision of offenders.\textsuperscript{544} Airport security is another prominent example.\textsuperscript{545}

\begin{itemize}
\item \textsuperscript{537} Aas, Gundhus & Lomell 2009, p. 6/7.
\item \textsuperscript{538} Section 2.3 discusses the E.U. lawmakers mistreatment of GSM; section 2.4 discusses digital certificates and HTTPS.
\item \textsuperscript{539} Meijer 2011, p. 107.
\item \textsuperscript{540} Aas, Gundhus & Lomell 2009.
\item \textsuperscript{542} Aas, Gundhus & Lomell 2009, p. 7.
\item \textsuperscript{543} Morozov 2013. Zedner, in Aas, Gundhus & Lomell 2009, p. 268-269.
\item \textsuperscript{544} Aas, Gundhus & Lomell 2009, p. 7.
\item \textsuperscript{545} Schneier 2003. Aas, Gundhus & Lomell 2009, p. 6/7.
\end{itemize}
These general observations on technology policy come into play in EU communications security policy. Recent work by Gürses on cybersecurity research funding discourses, for instance, suggests that the reframing of security and engineering and policy from goals such as ‘confidentiality’ and ‘privacy’ into the now prevalent goal of ‘resilience’ obscures crucial normative debates. When the goal of cybersecurity research and policy is resilience, a premium is put on the need for communications to be always-on. Availability as a goal is stressed, rather than communications confidentiality or integrity. The technical tools change in the process, from applying robust encryption to pervasive monitoring and filtering. Gürses hypothesizes that “if this reading of the new cybersecurity materializes, then it is unreasonable, if not illusory, to imagine that engineers can strike a balance between privacy and cybersecurity through the systems that they design.”

The reframing of communications and information systems security into cybersecurity and resilience, along with the prioritization of availability and continuity over confidentiality and integrity, has been occurring for years at the EU level. Perhaps intentionally, probably slowly, surely and unintentionally. Therefore, the EU lawmaker must always seek to open the black box of technology, engage with the complex technical underpinnings and concepts of communications security policymaking and strive for a transparent debate on its underlying norms and values. The case studies of Part III will also seek to illuminate the (possibly obscured) politics in the specific technology policy areas of HTTPS and ‘cloud’ communications security policymaking by the EU lawmaker.


547 Idem.

548 See, for instance, section 2.1 and 2.4. on critical infrastructure protection and digital certificates.
6.5. Conclusion

This study established that the political conception of security lies at the heart of the conceptual ambiguity regarding ‘security’ in EU law, signaled in Part I. In its political manifestation, security carries highly divergent meanings and often hidden agendas that are hard to resolve in EU law. In its most clear-cut manifestation, the Snowden disclosures around operation BULLRUN have demonstrated how national security is often diametrically at odds with technical security. Part I of the study already established that securitizing actors such as intelligence and law enforcement agencies are closely tied to the EU policymaking arena. Ongoing debates, especially in the ‘network and information security’ policy cycle, show not much sign of the EU being capable of overcoming these divergent understandings of security and the framing by Member States of communications security as a matter of national security. The political science perspective on EU communications security policymaking dynamics may lead to the viewpoint that technical communications security should not be legislated by the EU at all.

The fundamental rights perspectives of chapter 4 instruct that this trajectory is unacceptable. At the same time, at least theoretically, the lack of explicit competence to legislate matters of national security could be seen as an opportunity to re-orient EU policymaking towards a more objective, technical conception of security. The genuine fundamental rights, consumer protection, internal market and innovation interests associated with a secure networked communications environment fall squarely within the regulatory competence of the EU lawmaker. Many of the policy cycles of Part I do concern broader interests beyond national security, and impact communications security levels across the EU – particularly regarding a majority of non-technical users.
Chapter 6 concludes that the future trajectory of EU communications security legislation is closely tied to how it will be framed as a policy issue by the EU lawmaker. Apart from the Court, Commission and the Parliament, that legislature also includes the EU Member States, joined in the EU Council. Part I showed the strong influence of national security and law enforcement interests on EU communications security law so far. Still, many of the policy cycles identified in Part I are not directly or explicitly tied to the established sectors of securitization. The developments in the current ‘third phase’ of legislative action at the EU level across all five policy cycles, and a relatively young new institutional order of the EU adopting the EU Charter of Fundamental Rights, will prove whether the EU as a polity is capable of balancing competing interests in legislating communications security.
PART III: CASE STUDIES FOR THE EU LAWMAKER

7. Model and Methodology

Part I and Part II of the study researched the history, concepts and tools of EU communications security law. To further research the historical, constitutional, systems design and political perspectives offered so far, Part III of the study conducts two case studies on essential communications uses for every Internet end user: web browsing through HTTPS, and communications security in remote computing, better known by its marketing term ‘cloud’ computing. Ultimately, the case studies aim to assess the role of EU legislation in two specific communications uses. Finally, Part IV synthesizes the findings of the study to draw broader conclusions on how EU law should protect end user communications security.

The case studies follow the general research question, but replace private communications with the more specific subject matter of the case study at hand. The HTTPS and ‘cloud’ communications security case studies cover communications uses that each Internet user, perhaps unknowingly, is confronted with every minute spent online. The cases are interconnected: in chapter 8, the HTTPS case study examines systemic security vulnerabilities on the communications path between a user and a website operator. The case study produces an extensive market concentration analysis to examine the incentives to produce security in the market for HTTPS certificates. In chapter 9, the cloud communications case looks into similar issues on the communications paths within the data centers of large Internet companies: intradomain communications within the logical boundaries of Internet companies, as well as interdomain communications between intermediaries online. The systemic security vulnerabilities are analyzed through the lens of
surveillance incentives in operation MUSCULAR disclosed by Edward Snowden.

Both case studies use the same structure and conceptual framework to assess how EU law should protect end user communications security in these specific use contexts. The structure and conceptual framework of the case studies follows the general methodology of the study complemented with research methods from security economics, security requirements engineering and computer science. This leads to the formulation of a step-by-step model that organizes the subsection of the case studies, which is further informed by the findings in Part I and II:

1. Map the functional value chain of relevant communications uses;
2. Identify systemic vulnerabilities;
3. Analyze market and surveillance incentives;
4. Operationalize the c.i.a.-triad and fundamental rights perspectives;
5. Examine the available technical solutions;
6. Assess the role of EU law so far and offer recommendations.

The case studies have already been peer-reviewed in academic journals, conferences or discussed at workshops across relevant disciplines. All steps are followed in both case studies. The third step, uncovering market and surveillance incentives, needed a different approach in both case studies. HTTPS and cloud communications cover different communications uses and technologies, different functional value chains and thus stakeholders, and different root cause of the security failure. Step 3 of the HTTPS case study focuses on identifying market incentives and has an empirical bent towards security economics methods. The cloud communications case primarily analyzes operation MUSCULAR and thus focuses on surveillance incentives.

549 The first footnote of the case study chapters refers to these prior publications, conferences and workshops.
(section 9.3) and fundamental rights analysis (section 9.4), and to a lesser extent looks at their interplay with market incentives. Therefore, composition and threat modeling methods from computer science are applied as additional research methods. Using different methods for each case enables deeper analysis of the communications security issues at hand. Finally, in assessing the role of EU law so far, descriptive legal methods are used in both cases. The recommendations combine descriptive with normative legal analysis.
8. HTTPS – Communications Security in Web Browsing

Hypertext Transfer Protocol Secure (‘HTTPS’) has evolved into the de facto standard for secure web browsing. Through the certificate-based authentication protocol, web services and Internet users first authenticate one another (‘shake hands’) using a TLS/SSL certificate, encrypt web communications end-to-end and show a padlock in the browser to signal that a communication is ‘secure’. In recent years, HTTPS has become an essential technology to protect social, political and economic activities online. At the same time, widely reported security incidents – such as DigiNotar’s breach and OpenSSL’s Heartbleed – have exposed systemic security vulnerabilities of HTTPS to a global audience. And the Snowden revelations – notably around operation BULLRUN, MUSCULAR and the lesser-known FLYINGPIG program to query certificate metadata on a dragnet scale – have driven the point home that HTTPS is both a major target of government hacking and eavesdropping, as well as an effective measure against dragnet content surveillance when Internet traffic traverses global networks. HTTPS, in short, is an absolutely critical, but fundamentally flawed cybersecurity technology.

The 2011 security breach at a small Dutch Certificate Authority (CA) called DigiNotar was a watershed moment, demonstrating these theoretical man-in-the-middle vulnerabilities in the wild. Meanwhile, large CAs such as Comodo and Verisign have experienced breaches as well, but didn’t suffer similar consequences as DigiNotar. In fact, the case study will explain how large CAs including market leaders that suffered actual breaches benefited from the increased sense of HTTPS insecurity.

---

550 This case study is based on three earlier publications: Arnbak et. al. 2014; Asghari et. al. 2013; Arnbak & Van Eijk 2012. In phases, the text of this chapter can be identical to the text used in these papers. The research for the latest paper in the series was concluded in September 2014. The text has only been slightly updated in June 2015. Views and errors in the case study remain the sole responsibility of the author.
Policymakers and technologists are increasingly advocating various solutions to address the security collapse of HTTPS. The EU has adopted the first comprehensive legislation on HTTPS in the world. In the US, on the other hand, attention has focused on several technological solutions and industry self-regulation. To evaluate both legal and technical solutions, the case study subsequently examines the HTTPS value chain, the incidents and systemic vulnerabilities of the technology as demonstrated by the publicized breaches and the underlying values of HTTPS communications through the conceptual lens offered by the c.i.a.-triad. Next, the case study looks at the CAs and the market for SSL certificates. To better understand the security incentives under which they operate, the case study analyses several datasets of certificates for HTTPS traffic. This uncovers a surprising pattern: a highly concentrated market with very large price differences among suppliers and limited price competition. In light of the analysis on the security incentives of CAs, the case study discusses the regulatory and technical proposals to address the systemic vulnerabilities in the HTTPS value chain.

Essentially, HTTPS is a two-step process: first, using a combination of technical and organizational measures, a trust relationship (a ‘handshake’) is established between website operators and the web browser of an end-user, providing authentication. Secondly, successful authentication leads to a TLS/SSL encrypted channel between the website and browser (a ‘tunnel’).\(^{551}\) The case study focuses on communications security issues of the authentication model. The handshake authentication serves as the stepping stone for the confidentiality and integrity that HTTPS seeks to deliver.\(^{552}\) Several high profile incidents have emerged over the last years that provided the societal and scientific relevance to study it in depth, all discussed in the following sections.

\(^{551}\) Anderson 2008, p. 670.
\(^{552}\) Roosa & S. Schultze 2010, p. 3.
After the research for the case study was concluded, serious incidents in the second step of HTTPS – the tunnel itself – have emerged, including “Logjam” and “Heartbleed” that exposed security vulnerabilities in the commonly used encryption key exchange mechanism Diffie-Hellman and in encryption library OpenSSL used by all major HTTPS stakeholders. But as the associated actors, functional value chain, as well as market and surveillance dynamics differ substantially, the communications security issues evolving around the encrypted tunnel in HTTPS have not been included in this case study.

8.1. The HTTPS Communications Value Chain

This section describes the HTTPS Authentication Trust Model, the HTTPS market and the actor-based HTTPS Authentication Value Chain, in order to gain insight into the interactions between its key stakeholders. For a more extensive description, we refer to earlier work by two of the authors.

Current HTTPS Authentication Model

Hypertext Transfer Protocol Secure (‘HTTPS’) adds Secure Sockets Layer / Transport Layer Security (‘SSL/TLS’) technology over usual HTTP browsing on the World Wide Web. If a website or service wants to provide HTTPS, it needs to obtain an SSL/TLS certificate from a CA. Basically, these certificates are small computer files that might contain information on hostname (website), certificate owner (website), certificate issuer (CA), validity period and public key. The amount of information that SSL certificates provide depends on the type of certificate purchased by its owner. Domain Validated (DV) certificates can be acquired at low cost and may require a website operator to reply to an e-

554 Arnbak & Van Eijk 2012, Section 2.
555 Anderson 2008, p. 672.
mail sent by the CA to a standard e-mail address in the WHOIS database for domain validation. The various types of Organization Validated (OV) and Extended Validation (EV) certificates require more thorough validation by the CA, for example by phone, written letter or face-to-face, verifying both domain and the organization behind it – the end-point. If validation succeeds, CAs sign the OV or EV certificate.

Every time an Internet user visits a particular website, his browser requests the site to identify itself. The server of the website responds by either offering no information (standard unencrypted communications over HTTP) or a copy of its SSL certificate to the browser. If a browser receives an SSL certificate, it sets out to check if it trusts the issuing CA. In the case of untrusted CAs (or self-signed certificates that seek an SSL connection), the browser may give the end-user a security warning of an ‘untrusted connection’. If the browser does trust the issuing CA, it subsequently aims to prove that the public key assigned to the SSL certificate matches with the certificate of the issuing CA. If this second test succeeds, a chain of trust is established: through the SSL certificate issued and signed by a trusted CA, the browser trusts that the domain name and the server it directs to actually belong to the same entity. Browsers notify users of a successful handshake, either by displaying a padlock, or changing colors in the location bar or some other conspicuous area of their browser. The described data flows are visualized at the end of this section, after a brief description of the direct stakeholders in HTTPS communications.

*The Functional Value Chain*

Since the inception of the HTTPS authentication process with the advent of the Netscape browser in the 1990s, a vibrant market for HTTPS communications emerged. This market involves roughly four direct stakeholders: i) website operators; ii) certificate authorities; iii) web browser vendors, and iv) end users.559

Website operators decide whether to deploy HTTPS or not. Deploying HTTPS may be achieved at low costs and sends out a message that end-users can entrust the website with valuable information, such as personal data, private communications and financial transactions. A notable drawback for website operators to deploy HTTPS is that embedded content – third party ads, feeds, widgets and tracking networks – may not support HTTPS, in which case the advantages of HTTPS are lost. So if embedded content is a part of the revenue model of a website operator, which is the case with many websites, it has strong incentives not to deploy HTTPS.561

HTTPS deployment is not a binary affair, in the sense that a website provides it, or does not. Website operators have many options for implementing HTTPS that have a consequent impact on the level of security provided. Vratonjic et al. found that ‘only 16% of the websites implementing HTTPS carry out certificate-based authentication properly’. 562 SSL Pulse, a project run by

559 Roosa & Schultze 2010, p.4. Subscribers is a somewhat broader and more accurate term for website operators, as buyers of certificates do not necessarily have to be website operators. For ease of reading, this paper will use the terms websites or website operators.

560 See <https://support.google.com/adsense/bin/answer.py?hl=en&answer=10528>, accessed 2 September 2015.


562 Vratonjic 2011, p.3: “i.e. using trusted, unexpired certificates with valid signatures, deployed on proper domains.”
security firm Qualys, finds that only 13% offer end-users (what Qualys calls) ‘genuine security’, only 8% use EV certificates and less than 1% support the HTTP Strict Transport Security protocol, in effect forcing browsers to communicate with the site through HTTPS. These numbers support the claim that the state of HTTPS implementation is sub-optimal from a security perspective.

Certificate Authorities sell certificates and exist, broadly, in three categories: Root CAs, intermediate/subordinate CAs and untrusted CAs. Root CAs are trusted by default by browsers, after they have solicited for such a status with the browsers and complied with the varying browser CA trust policies. Intermediate/subordinate CAs are either directly verified by one Root CA or part of a chain of trust of several intermediate CAs that ultimately ends with one Root CA. Interestingly, both Root CAs and intermediate CAs that are part of such a chain of trust are treated equally by browsers, leading to a successful authentication. Untrusted CAs or self-signed (by the owner of a website) certificates evoke the ‘untrusted connection’ security warning when they offer browsers an SSL connection.

A crucial technical property of the HTTPS Authentication Model is that any CA can sign SSL certificates for any domain name. This ability to sign for any domain name has profound implications for the security of the HTTPS ecosystem. For example, a domain name holder – say Google in the case of www.google.com – possesses an SSL certificate for his domain. This doesn’t stop anyone in stepping to any CA and requesting another SSL certificate for

---

564 From the SSL Pulse website: “To be secure, a site has to be well configured, which means that it must have the A grade. In addition, it must not be vulnerable to any of the two currently known attacks against SSL (Insecure Renegotiation and the BEAST attack).” See <https://www.trustworthyinternet.org/ssl-pulse/>, accessed 2 September 2015.
565 Soghoian & Stamm 2011, p. 2.
www.google.com, even though this other CA is not the CA that Google approached to sign its SSL certificate. From the CA perspective, there are institutional limits to issuing this particular certificate (validation procedures), but no technical ones. So if one obtains this second certificate with a CA that has root status, browsers will react by trusting the second certificate by default. End-users will get the familiar HTTPS notification, without noticing whether their HTTPS communications are mediated by the Google-owned certificate or the second certificate.

From a business perspective, however, the position in the ecosystem and the fact that CAs can sign for any domain name is attractive.\textsuperscript{567} The CA industry has flourished over the last decade, as it is relatively easy to set up your own CA and buy yourself into a chain of trust.\textsuperscript{568} Many root CAs own multiple subordinate CAs that may partake in such a chain of trust and in that case enjoy default trust by browsers. According to many observers, this practice enables root CAs to divide operations in various market segments and compete with other CAs on price differentiation, as many websites don’t seek high security certificates, but cost-effective ones.\textsuperscript{569} From our empirical research and analysis of HTTPS market characteristics in Section 5 and 6, we will actually conclude that this is not the case.

\textit{Web browser vendors} serve as the interface between website owners, CAs and the end-user. In particular, the HTTPS ecosystem relies upon browsers to establish whether a particular CA can be entrusted root status and to check the validity of certificates. Furthermore, it notifies successful authentication and

\textsuperscript{567} Roosa & Schultze 2010, p. 4 and footnote 8-10. There are numerous webpages that describe how to become a CA around, for example: <http://technet.microsoft.com/en-US/library/ff849263%28v=ws.10%29.aspx>, accessed 2 September 2015.
\textsuperscript{568} Roosa & Schultze 2010, p. 3.
\textsuperscript{569} Roosa & Schultze 2010, p. 6; Vratonjic 2011, p. 31/32.
the establishment of encrypted tunnels to the end-user. In determining whether CAs should be granted root status, browsers have developed different trust policies. This leads to a different number of root CAs per browser. We return to this in section 5.

In the case of (or if there is reason to suspect) certificate or even CA compromise, swift trust revocation is essential to minimize the associated risk. For certificates, all major browsers employ Online Certificate Status Protocol (OCSP) responders. These are operated by CAs and let browsers check whether trust in a certain certificate has been revoked. For CA revocation, browsers need to alter aforementioned root CA lists and patch the browser software, which end-users subsequently need to update to take effect. An important drawback of OCSP effectiveness is that its use by CAs is not mandatory and often overruled in order to maintain connectivity between a web service and users.

End users have an interest in seeking HTTPS communications with websites, as it is their valuable information that is on the line. However, users depend to a large degree on security decisions made by the aforementioned stakeholders. Websites initiate HTTPS communications through SSL certificates, which are validated and signed by CAs and verified by browsers. End users don’t interact directly with CAs. Only a very small margin of technically savvy users might

570 The notification depends on the type of browser the end-user has installed on his device. The notifications vary from browser to browser, making it difficult for the average user to recognize succeeded authentication and make decisions-making on pursuing the connection with that particular website. See <https://freedom-to-tinker.com/blog/sjs/firefox-changes-its-https-user-interface-again/>, accessed 2 September 2015.

pursue an (indirect) relationship with CAs through browser preferences, for example by blocking all certificates provided by a certain CA.\textsuperscript{572}

A common practice for CAs is to disclaim liability for losses suffered as a cause of reliance in certificates.\textsuperscript{573} Roosa & Schultze observe that CAs ‘place onerous technical obligations […], such as being familiar with cryptographic protocols and making independent judgements about the trustworthiness of any given digital certificate’ on end-users.\textsuperscript{574} And with self-signed certificates, even though they might be very securely implemented, a browser might issue a warning of an untrusted connection, making it even harder for the average end-user to assess the security of a connection. In this context, the average end-user cannot reasonably be expected to exert control over the HTTPS ecosystem.\textsuperscript{575}

Now that the authentication process, its data flows and the HTTPS market have been described conceptually, the functional value chain for the HTTPS ecosystem can be mapped. This communications security value chain helps to understand the broader interactions at stake throughout the ecosystem, rather than the market incentives of one particular stakeholder alone.

The data flows and functional value chain of HTTPS communications are visualized below:\textsuperscript{576}

\textsuperscript{572} ENISA 2011, p. 2. In particular footnote 5, which refers to the New Zealand BankDirect case, in which 299 in 300 users dismissed security warnings. Also Vratonjic 2011, p.32.
\textsuperscript{573} Vratonjic 2011. Roosa & Schultze 2010, p. 6. We will return to recent developments on liability issues in our analysis of the CA/Browser Forum initiatives in paragraph 4.
\textsuperscript{574} Roosa & Schultze 2010, p. 7.
\textsuperscript{575} ENISA 2011, p. 2. With regard to privacy policies, research shows that 1 in 1000 end-users click on the policy tab, spending an average 5 seconds on the page. Y. Bakos et al., ‘Does Anyone Read the Fine Print?’, CELS 2009 4th Annual Conference on Empirical Legal Studies, p.2.
\textsuperscript{576} Figure taken from Arnbak et. al. 2014.
8.2. Incidents and Systemic Vulnerabilities

On Friday 2 September 2011, a nocturnal press conferences of the Dutch Minister of Internal Affairs marked the beginning of the DigiNotar affair, which ultimately resulted in the CA’s bankruptcy. The affair was triggered by unauthorized access, reportedly by a hacker sympathizing with the government of Iran in mid July 2011, to the root CA capacity of DigiNotar. Three months later, it emerged that in this long period of obscurity, 531 false certificates had been created, the non-exhaustive list of which is quite alarming: Google, Facebook, Skype, Microsoft update, the CIA, Israeli intelligence service Mossad, and many others. DigiNotar had root status with all major browser vendors, so all these corrupt SSL certificates would have been trusted

---

578 Fox-IT 2011, p. 10.
by default. What is known today, is that the attacker abused the *.google.com certificate on a large scale, eight other certificates unknown on a small scale and the login.yahoo.com certificate to check whether a successful attack could be performed.\footnote{Fox-IT 2012, p. 62-63.} It is possible that other rogue certificates were used, but the forensic experts weren’t able to confirm or deny this, as the attacker had the capability to tamper with the DigiNotar log files.

The forensic report illuminated that DigiNotar failed to implement basic security measures. Thirty critical updates had not been performed, logging was insufficient (as discussed above) and DigiNotar had no anti-virus protection in place at the time of the intrusion.\footnote{Rb. Den Haag, 30 jul. 2014, ECLI:NL:RBAMS:2014:4888 (Diginotar).} Moreover, all (qualified, root and subordinate) CA servers were members of the same Windows domain secured with a weak password (Pr0d@dm1n).\footnote{Fox-IT 2011, p. 8-9. The physical security was in perfect state, peculiarly, as the servers stood in highly expensive a tempest proof room.} Interestingly, DigiNotar complied with existing regulations and had successfully passed several ESTI standardized periodic auditing procedures by renowned accounting firms for the issuance of EV certificates and Qualified signatures.\footnote{From ENISA 2011, p. 1: “DigiNotar was audited yearly by an independent auditor against the ETSI standard (TS101456) for certificate authorities” and p. 2: “The DigiNotar website until recently showed an audit report stating that “the management system for issuance of certificates of DigiNotar complies with ETSI TS 101 456 (v. 1.4.3) - normalized certificate polices NCP+, EV specified in ETSI TS 102 042 (v. 2.1.2).”}

The damage was probably enormous, but cannot be determined with certainty due to the unreliability of the log files. Based on the logging of OCSP requests at DigiNotar, the HTTPS communications of reportedly 300,000 different, mostly Iranian IP-addresses were intercepted.\footnote{Fox-IT 2011, p. 8. But this number is contentious, as OSCP requests are not mandatory, and could have been blocked or even faked by the attackers.} ENISA speaks of ‘millions of citizens’ and notes that some experts believe that the lives of Iranian activists
have been put at risk.\textsuperscript{584} In addition, investigators could not rule out the possibility that undetected rogue certificates were used in the Qualified and PKI Overheid environments.\textsuperscript{585} Therefore, the entire range of DigiNotar activities could have been compromised and could no longer be trusted.

Comodo, a market leading CA, suffered several security breaches.\textsuperscript{586} The best documented breach regarding Comodo was the compromise affecting its ‘UTN-USERFirstHardware’ certificate. According to data analysis from its SSL observatory, EFF calculated that ‘85,440 public HTTPS certificates were signed directly by UTN-USERFirst-Hardware. Indirectly, the certificate had delegated authority to a further 50 Certificate Authorities, collectively responsible for another 120,000 domains.’\textsuperscript{587} Notably, EFF reports that the Comodo breach was discovered through smart cross-referencing of browser security updates by security researchers, rather than notification by the CA itself.\textsuperscript{588}

Verisign, another market leading CA, was hacked in 2010. The breach was only discovered by news agency Reuters in February 2012,\textsuperscript{589} after Security and Exchange Commission regulations mandated companies to notify investors of

\textsuperscript{584} ENISA 2011, p. 2.
\textsuperscript{585} Fox-JT 2011, p.9. Around the time of the breach, millions of Dutch citizens submitted their income tax forms to the Dutch tax administration bureau, with 1 September as a deadline. It goes beyond the reach of this paper to fully research the implications of this fact, but it is a striking example of the amounts of sensitive information DigiNotar certificates were a crucial link in protecting. Still, in August 2012, tax advisors are using DigiNotar certificates for making submissions to the Dutch Tax office, see <http://www.rijksoverheid.nl/ministers/fin/nieuws/2012/07/23/belastingdienst-waarschuwt-adviseurs-die-nog-gebruik-maken-van-diginotar-certificaten.html>, accessed 2 September 2015.
\textsuperscript{588} Jacob Appelbaum and other security experts at the TOR Project, whose analysis on the cross-referencing is highly recommended. See <https://blog.torproject.org/blog/detecting-certificate-authority-compromises-and-web-browser-collusion>, accessed 2 September 2015.
\textsuperscript{589} See <http://www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202>, accessed 2 September 2015.
intrusions since October 2011.\textsuperscript{590} Apparently, administrators within Verisign had kept the breach silent, even from their own top management. According to the Reuters reports, a former CTO claimed he had not learned of the intrusion until contacted by Reuters and said Verisign ‘probably can’t draw an accurate assessment’ of the damage, ‘given the time elapsed since the attack and the vague language in the SEC filing’. Verisign, meanwhile, claimed that ‘there is no indication that the 2010 corporate network security breach […] was related to the acquired SSL product production systems.’\textsuperscript{591}

From extensive public reporting on DigiNotar, we know that the CA had extremely poor security practices, which led to a landslide breach. The breach at CA GlobalSign, yet another market leading CA, is another example of poor security practices, as software running on a public-facing webserver was not updated. Information on the breach is limited, however, as the public only found out about the nature of this breach from an interview given by a company representative months after.\textsuperscript{592} Technically, CA Trustwave did not suffer a breach. However, it became public that it had used its root CA status to enable third parties to issue SSL server certificates for employee monitoring purposes. Trustwave subsequently claimed that this is common practice among other root CAs.\textsuperscript{593} Regardless if this claim is true or false, it illustrates the compelled-CA attack of Soghoian & Stamm in real life: CAs are in a unique position to enable surveillance of end-users.\textsuperscript{594} This section has not covered all

\textsuperscript{594} Soghoian & Stamm 2011.
publicly known CA breaches, but a pattern of vulnerabilities emerges nonetheless. Regardless of scale, CAs get breached. They are reluctant to inform both relevant authorities, customers and the general public (end-users) about these breaches. Security practices at DigiNotar and GlobalSign proved to be below a ‘state of the art’ or ‘general industry practice’ level, while this cannot be established for the breach at Verisign and the multiple Comodo breaches.

Currently, there is no way of knowing whether larger CAs are more secure than small CAs as an organization, and if the certificates issued by large CAs are more trustworthy than those of small CAs. Given the weakest link concerns throughout the HTTPS ecosystem, the crucial question that emerges is, why was trust in the entire CA practice of DigiNotar revoked by the web browser vendors, while larger CAs dodged the bullet?

ENISA argued in the aftermath of the DigiNotar breach that if a larger CA were to suffer a similar security breach, trust revocation by browser vendors in its certificates would seriously impact web communications on a global scale: ‘it can even be argued that CAs of this size are too large to fail.’ In the event of a revocation of Comodo in the aftermath of a breach, trust revocation would render all the HTTPS servers that use the certificates of this large CA untrustworthy, in effect leaving the websites inaccessible. The Electronic Frontier Foundation (EFF) describes this dilemma for web browser vendors as follows:

595 Roosa & Schulze 2010, p. 5 report on other breaches. Furthermore, KPN/Getronics, StartSSL TurkTRUST and several other CAs have been breached in recent years.
596 ENISA 2011, p. 2.
‘browsers would face a horrible choice: either blacklisting the CA quickly, causing outages at tens or hundreds of thousands of secure websites and email servers; or leave all of the world’s HTTPS, POP and IMAP deployments vulnerable to the hackers for an extended period of time.’

DigiNotar, then, was only a small player in the HTTPS market employing poor security practices and not being frank about them when it discovered that its systems had been breached. The decision to revoke trust in this small CA must have been less ‘horrible’ than in the case of Comodo, GlobalSign or Verisign – irrespective of their practices.

**Systemic Vulnerabilities**

*Weakest link.* The fact that any CA can vouch for any domain name, then, is probably the most important and widely recognized vulnerability. This makes each of the hundreds of CAs in over fifty jurisdictions a weakest link for potentially all HTTPS communications. As ENISA observes: ‘The security of HTTPS equates to the security of the weakest CA.’\(^{598}\) The scenarios for failure are manifold: any CA could facilitate or be a malicious actor engaging in cybercrime, or be a company monitoring its employees, or could be compelled by a state actor to enable mass surveillance of Internet users,\(^{599}\) or one of its administrators could simply have a bad day – forgetting updates, writing poor code or in his own right be coerced to cooperate in malicious activities.

*Non-forensic auditing obligations.* The weakest CA known to date, DigiNotar, passed the mandatory periodic audits, both the ones based on Dutch regulation for qualified certificate issuers and those based on internationally recognised industry standards. As successful audits negotiate CA root status by web

---

\(^{598}\) ENISA 2011, p. 2

\(^{599}\) Soghoian & Stamm 2011.
browsers, all major browsers trusted DigiNotar by default – irrespective of its poor security standards. In the case of DigiNotar, the CA consequently failed to devise and implement basic security policies for years, even though forensic audits have warned for serious vulnerabilities since 2006 – over three years before the public learned of the devastating breaches in 2009. The perceived security that the current ‘paper trail’ auditing obligations should deliver is another systemic vulnerability of HTTPS.\(^{600}\)

Information asymmetry. The recurring information asymmetries are another striking systemic vulnerability. Organizations – including CAs and website operators – have strong incentives to conceal poor security practices and breaches. The reputational damage can be harmful, especially when trust is a selling point. If we look at CAs, which have structurally failed to inform both browsers and the public about breaches, a breach risks not only the trustworthiness of the entire ecosystem, but also renders trust of end-users unjustified: end-users may disclose highly sensitive information based on erroneous assumptions of security.

Too big to fail. From the viewpoint of web browser vendors, the interests of providing connectivity versus assuring trustworthiness may conflict. This is demonstrated in the overruling of OCSP responses and in browser management of root status. If a major CA is breached or trust in a widely used certificate is revoked, the damage from a communications security perspective may be all the more alarming, but browsers face the hard choice of rendering a large part of the HTTPS encrypted web inaccessible to its end-users. If ENISA notes that major CAs are too big to fail, the weakest link phenomenon is even more worrying. In other words, CA scale is a risk vector when it comes to security: a

\(^{600}\) Roosa & Schultze 2010, p. 3.
breach may compromise more communications, but revocation is more complicated.

These conceptual considerations provide guidance into empirical research of the security incentives in the HTTPS certificate market in section 8.4. First, the case study describes the underlying values of HTTPS communications in the next section.

8.3. Incentives

The value chain analysis and discussion of systemic vulnerabilities provides a framework for empirical analysis of the HTTPS market, to provide a better understanding of the security incentives at play. It is only in light of such data-driven findings that one can start to reflect on the need for legal and technical interventions in the current HTTPS ecosystem. The empirical analysis focuses on security incentives in the market of the HTTPS authentication model, rather than surveillance dynamics that have emerged from several Snowden disclosures. The latter are discussed in more detail in the case study on ‘cloud’ communications in chapter 9.

Several studies have surveyed the SSL certificate market. Two of the largest have been the EFF SSL Observatory in 2010 \(^{601}\) and the University of Michigan's HTTPS ecosystem scans in 2012-2014. \(^{602}\) Both projects systematically scanned the entire IPv4 address space, looking for public facing HTTPS servers. They retrieved the SSL certificates presented by these servers and later parsed and validated them to determine whether different browsers and operating systems would trust that certificate.

---

\(^{601}\) See <https://www.eff.org/observatory>, accessed 2 September 2015.
\(^{602}\) Durumeric et. al. 2013.
The first version of this case study used the EFF data set, which contains approximately 1.5 million trusted certificates, in empirically establishing the number of CAs, the firms that own them, their market shares, and the pricing strategies. A second, updated version of the study compares these findings against the HTTPS ecosystem scan data set, which has approximately 3 million trusted certificates. While the latter scan has collected more certificates than the EFF data set, this difference mostly reflects a linear growth pattern over time in the number of certificates in use on the Web, and to a limited extent improved scanning methodology. There is a difference of 400,000 certificates if the growth trend in the ecosystem scan data is extrapolated back in time to the EFF data-collection period. Despite these differences, the following patterns are consistent across both data sets.

Many CAs. Foremost, the number of organizations that can issue browser-trusted certificates is high. There are between 1,000 and 2,000 trusted CAs, including root and intermediate CAs. Multiple CAs might be owned by the same organization for a variety of operational and business needs, so the number of issuing organizations is lower. Mapping CAs to organizations leads to an estimated 250 to 700 trusted certificate-issuing organizations, located in 57 countries worldwide. Heterogeneity is often good for an ecosystem, especially in terms of resilience. Because of the weakest-link nature of the HTTPS system, however, this also means many more single points of failure in case of CA compromise or misconfiguration. What's particularly troubling is that a number of the trusted CAs are run by authoritarian governments, among other less trustworthy institutions. Their CAs can issue a certificate for any website in the world, which will be accepted as trustworthy by browsers of all Internet users.

---

603 Asghari et. al. 2013.
604 Arnbak et. al. 2014.
HTTPS market concentration. Second, the market for SSL certificates is highly concentrated, despite the large number of issuers. In fact, both data sets find that around 75 percent of SSL certificates in use on the public Web have been issued by just three companies: Symantec, GoDaddy, and Comodo. Symantec, the largest commercial CA, owns multiple brands, including Verisign, GeoTrust, Thawte, RapidSSL, and TC TrustCenter. The distribution is heavily skewed, with smaller CAs having little or no presence on the public Internet. Power-law distributions, although not surprising in Internet service markets, pose a major risk for the HTTPS ecosystem: if one of the large CAs is compromised, its root status cannot be revoked by browser vendors without massive collateral damage. One particular CA of GoDaddy had signed 26 percent of all valid HTTPS certificates in March 2013. That means if it were compromised, 26 percent of all websites that rely on HTTPS would need to be immediately issued new certificates.\(^9\) Otherwise, browsers ought to present certificate warnings or block access to those sites, posing an impossible tradeoff for the user between access and security. In other words, such large CAs are truly "too big to fail."

Weak price competition. Mapping the prices for different certificate brands provides a sense of the degree to which the market is dominated by price competition. The figure below shows the price and market share for DV certificate offerings.\(^{605}\) Symantec/GeoTrust certificates (e.g., QuickSSL Premium) sell for $149 but have a much larger market share than Gandi SSL certificates selling at $16:

---

\(^{605}\) Taken from Arnbak et. al. 2014.
The situation is extreme in the EV market, as shown in the figure below. The market leader, Verisign, sells certificates for approximately $1,000 and has a 63 percent market share. GoDaddy, offering certificates at a fraction of that price ($100), captures a mere 5 percent of the market. The differences are intriguing, as certificates themselves are perfect substitutes (within each validation category). The differences might be explained by features bundled with the certificates, discussed in the next section. In sum: the SSL market shows few signs of intense price competition.

Taken from Arnbak et. al. 2014.

These comparisons have certain limitations, most notably that prices are as advertised by vendors in March 2013, while market shares were from the EFF 2010 data set. The more recent and longitudinal HTTPS ecosystem scan data shows that similar market shares hold over time, with a slight shift of a few percentage points away from Symantec to cheaper providers.

---

606 Taken from Arnbak et. al. 2014.
607 These comparisons have certain limitations, most notably that prices are as advertised by vendors in March 2013, while market shares were from the EFF 2010 data set. The more recent and longitudinal HTTPS ecosystem scan data shows that similar market shares hold over time, with a slight shift of a few percentage points away from Symantec to cheaper providers.
Analysis of HTTPS Market Incentives

Security economics often claims a race to the bottom exists in security markets: a market dominated by fierce competition pushing prices toward marginal cost, with perverse incentives for security.\(^{608}\) Various researchers and industry observers have claimed that such a race to the bottom exists in the HTTPS market to explain for the poor security practices at DigiNotar and other compromised CAs.\(^{609}\) Indeed, at first glance one would indeed expect such a race. Certificates are perfect substitutes, suggesting a completely commoditized market. Also, buyers can't meaningfully distinguish secure from less secure offerings; and even if they could, buying from a more secure CA cannot protect


the site owner against the threat of an attacker fraudulently signing the domain with a certificate from a compromised CA.

The empirical data, however, clearly suggests otherwise, showing market concentration and little price competition. In one sense, it is good news that the market is not driven by a race to the bottom, given the perverse security incentives associated with such a race. Rather than certificates themselves, however, the HTTPS market is driven by:

- Bundled security services such as scans of the buyer’s site for malware.
- Enterprise certificate management services such as support for management and billing of large numbers of certificates.
- Brand reputation as a liability shield against shareholders, regulators, or others who may hold the buyer accountable in the face of security issues.
- Trust or security signals aimed at third parties and end users such as site seals, warranty amounts and the high price of a certificate itself.
- Higher continuity in case of security failures at the CA, because of the too-big-to-fail dynamic of market-leading CAs.

Knowledgeable buyers understand that security in this market is a weakest-link problem and thus determined by the weakest CA. They also understand that three of the four market leaders got hacked in recent years and that some of the ‘security’ features of these services do not really provide actual security. Nonetheless, buying from the market leaders is still rational, given the liability shield and higher continuity. The price differences are not enough to outweigh these advantages. They may be large in a relative sense, but they are modest in absolute terms, compared with other cost components in large firms.

610 See more extensively in Ashgari et. al. 2013.
Given that the market leaders successfully differentiate their products via, among other things, security-related features, buyers appear to be willing to pay for security. Two classic problems, however, as mentioned before under the systemic vulnerabilities under section 8.2, affect the proper alignment of incentives in the HTTPS market:

- **Information asymmetry** prevents buyers from knowing what CAs are really doing. Buyers are paying for the perception of security, a liability shield, and trust signals to third parties. None of these correlates verifiably with actual security. Given that CA security is largely unobservable, buyers’ demands for security do not necessarily translate into strong security incentives for CAs.

- **Negative externalities** of the weakest-link security of the system exacerbate these incentive problems. The failure of a single CA impacts the whole ecosystem, not just that CA’s customers. All other things being equal, these interdependencies undermine the incentives of CAs to invest, as the security of their customers depends on the efforts of all other CAs.

The most powerful incentive for security seems to be reputation effects, but this does not necessarily make them more sensitive to the reputation damage caused by breaches. While they have more to lose compared with smaller brands, large CAs are less threatened by the ultimate reputation effect: being removed from the root stores.

Ironically, the security problems that have plagued the HTTPS ecosystem over the past few years, including the breaches at market leaders, may in fact benefit these same market leaders. The breaches have increased the demand for security, and this demand seems to latch onto whatever security signals are
available, regardless of their relationship to actual security. All of this may impact the attempts to fix the systemic vulnerabilities of the system. The dominant players might be reluctant – or less eager – to push for adoption of one of the proposed technological solutions. This is not to suggest that market leaders will act against them, but rather that the status quo works quite well for them.

In sum, the case study found that the market is highly concentrated, with very large price differences among suppliers and limited price competition. Market leaders differentiate their offerings partially via security features: their reputation enables them to offer security signals – though some of these signals are absurd and none of them correlate verifiably with actual security – and a limited liability shield. In other words, the current vulnerabilities may actually benefit rather than hurt the dominant CAs. These empirical findings run counter to what security experts had been warning about for years, a price and later security devaluation, or a so-called ‘race to the bottom’.

8.4. The c.i.a.-Triad in HTTPS

The underlying values and conflicting security goals of HTTPS can be described using the conceptual framework developed in Part II of the study. By deploying the c.i.a.-triad and specifying the conflicting interests at stake, several tensions emerge that need to be resolved through policymaking in order to augment HTTPS security.

Web browsing constitutes a central element in electronic communications for each and every end user. Its security is vital to the protection of fundamental rights, the economy, provision of public service and so forth. So far, fundamental rights safeguards have not determined predefined minimum
safeguards that needed to be taken into account in the dynamics after serious communications security breaches. Fundamental rights analysis does not come into play, perhaps with the exception of cases that evidently and directly relate to the processing of sensitive personal data. While TLS-certificates themselves perhaps do not contain such information, HTTPS itself is a major cybersecurity technology that protects massive amounts of communications and data against security breaches. In various highly sensitive communications use cases, HTTPS serves as the most important measure to protect communications confidentiality and integrity. Especially in the case of the DigiNotar breach, the communications of hundreds of thousands Iranian citizens and even the lives of Iranian activists apparently were at stake. Until today, the Dutch government heralds its handling of the breach as a huge success and exemplary case of the viability of public-private partnerships.\(^\text{611}\) Even if large economic damages were suffered, and no one exactly knew the implications of immediate revocation for the functioning of medical devices, traffic control and so forth, the dire consequences of confidentiality and integrity breaches go unmentioned.

The aftermath of the DigiNotar incident provides the most comprehensive material to date to illuminate these tensions in the real world, after a serious security incident. Web browsers vendors had to face the choice whether or not to revoke their trust in the root and intermediary capacities of the CA. Rather than displaying a website, trust revocation generates an alarming security warning in the browser for websites offering certificates signed by that particular CA (breach of ‘availability’). Refraining from trust revocation may expose websites and end-users to eavesdropping (breach of ‘confidentiality’) or modification of their communications (breach of ‘integrity’). A security breach at a market leading CA puts confidentiality interests of millions of websites and end-users at risk, far surpassing the reach of small CAs. On the other hand,

revoking trust of a large CA implicates the availability of a substantial part of the HTTPS-encrypted web. Web browser vendors are left with a difficult choice: either prioritize communications availability of websites, or confidentiality interests of end-users. Web browsers face a trade-off between their private interests to connect millions of Internet users per second, or protect their confidentiality and integrity interests.

In real life, the incident response dynamics in the aftermath of these breaches have revealed that the security goals of the web browser vendors were not formulated in a transparent way. In addition, HTTPS communications have by and large been unregulated throughout the world, so the decision of web browser vendors has not been informed by legal obligations. In the end, web browsers have all revoked the trust in the small CA DigiNotar, while not punishing market leading CAs in a similar way post-breach. Apparently, web browser vendors have prioritized the availability of websites over confidentiality interests of users.

A Fundamental Rights Perspective on HTTPS

Applying the CJEU Digital Rights Ireland framework, HTTPS mediates enormous information quantity and sensitivity, while the risks of abuse in a systematically flawed functional value chain with deeply conflicting interests are substantial. HTTPS, in addition, serves as the only ‘objectified’ first line of defense when communications traverse global networks between a website or service operator and end users. The whole point of deploying HTTPS over unprotected HTTP browsing communications is to provide added assurances of communications confidentiality and integrity over availability of such communications. It is a critical measure to protect against arbitrary national security interferences, as becomes clear in the next case study on ‘cloud’ communications.
In addition, one of the core concerns in the *ECtHR I. v. Finland* case was the lack of positive obligations to maintain the integrity of data security. Access to the health data was not under sufficient control before data were possibly breached, nor were logs kept to enable examination of access after the fact.\(^{612}\) In HTTPS communications, not only was Diginotar negligent in terms of its own systems, but the negligence of Diginotar effectively eliminated assurances as to the integrity (and confidentiality) of HTTPS communications as a whole for an extended period of time. For months, and even a week after the breach was publicized, it was more or less a wild west of surveillance on the encrypted web. The same holds true for the other incidents described in section 8.2., albeit it to lesser extent. In any event, strict integrity and confidentiality assurances are critical to not only protect the communications security of Diginotar-customers, but of users around the world.\(^{613}\)

In sum, from a fundamental rights perspective, HTTPS deserves particularly strict protection and explicit minimum safeguards from the constitutional and statutory lawmaker.

### 8.5. Technical Solutions

A host of technological solutions to the systemic vulnerabilities of the current system are being developed. Among the most prominent are Convergence,\(^{614}\) Perspectives,\(^{615}\) DANE,\(^{616}\) Sovereign Keys,\(^{617}\) Certificate Transparency,\(^{618}\) Public

\(^{612}\) See section 4.2.

\(^{613}\) In addition to the constitutional perspectives described here, prioritizing confidentiality and integrity in HTTPS communications also strongly resonates with the new IETF definition of communications security and other consensus documents on communications security released by the engineering community since the Snowden disclosures. See section 5.2.

\(^{614}\) See <http://convergence.io/details.html>

\(^{615}\) See <http://perspectives-project.org/>

Key Pinning,619 and TACK.620 From the perspective of governance, several general observations can be made:

- All proposals attempt to solve the weakest-link problem by introducing another authority to check whether the certificate that is validated through the normal HTTPS process is indeed the correct one.
- All proposals reduce the information asymmetry of buyers and users, versus the CAs, by systematically uncovering suspect certificates.
- All proposals can function on top of the current CA system, leaving it in place or depending on it; a subset can also replace it.
- All proposals can follow incremental adoption paths (albeit some are a lot more difficult than others), and all need support from browsers.

The proposals seem promising in terms of addressing the current weaknesses, especially the weakest-link problem, for which regulatory solutions appear ineffective. Therefore, in the long run they are preferable, and it's relevant to assess how they relate to the incentives of the HTTPS stakeholders. Some scholars predict that multiple proposals will eventually be adopted.621

None of these solutions, however, is close to large-scale adoption. As argued earlier, the insecure status quo can be beneficial for market leaders. In light of this, one might assume that CAs are not particularly keen on actively helping any of these proposals along, especially the ones that theoretically could make them obsolete. In practice, however, some CAs are involved in developing potential solutions—for example, DigiCert and Comodo are experimenting

---

617 Electronic Frontier Foundation, 2011, see <http://www.eff.org/sovereign-keys>
621 Bonneau 2013.
with Certificate Transparency.\textsuperscript{622} Other proposals require nontrivial activities on
the part of the domain owner, which may be done by their CA as a
complementary service to current business models.

Furthermore, each proposal is intensely debated in relation to browser
performance. Any form of large-scale adoption requires default support by
browser vendors. Google and Mozilla have been particularly active in this area.
While none of these solutions is easy to scale, there are benefits for early
adopters, a key requirement for any solution to take off. Whether the costs are
worth it depends on the kinds of threats HTTPS stakeholders want to defend
themselves against. An average cybercriminal might not be interested in
breaching a CA and manipulating network traffic already encrypted through
HTTPS, as financially attractive information can be acquired through more
cost-effective attacks.\textsuperscript{623} From previous breaches, it appears that state-
sponsored attackers and large corporations, rather than profit-driven criminals,
are more likely to engage in the complex man-in-the-middle attacks in the
realm of HTTPS. For some user groups and domains, such adversaries make
early adoption attractive.

Finally, a new CA was announced in mid-2014 called Let’s Encrypt. Initiated
by the Internet Security Research Group, a public benefit organization that
includes the support of a.o. the Electronic Frontier Foundation, the Mozilla
Foundation, Akamai and Cisco, the new CA aims to offer simple, automated
and free certificates for anyone. By June 2015, Let’s Encrypt had created its
Root and Intermediate CA capacities, but had yet to be launched. The prospect
of an open CA that offers easy-to-use certificates at no costs seems likely to

\textsuperscript{622} Langley 2012.
\textsuperscript{623} Florencio & Herley 2011. See also A. Langley, \textit{Real World Crypto 2013}, ImperialViolet
have an impact on HTTPS market dynamics, but could not be assessed when this case study was concluded.624

8.6. Current and Proposed EU Legislation

To improve the governance of HTTPS, the EU and the US have opted for a different approach. The US lawmaker entrusts augmenting HTTPS security to protocol innovation and lets industry self-regulate in the meantime.625 The EU, on the other hand, adopted comprehensive legislation to update the 1999 EU Digital Signatures Directive.626 The HTTPS authentication model had by and large been unregulated in both the US and the EU up until August 2014 when the EU adopted the eIDAS Regulation.627

The EU Commission initiated the updated legislation with a proposal for a Regulation in 2012. The potential influence of the CA breaches is not made explicit in the proposal nor in its accompanying documents. But earlier responses of the European Commission to parliamentary questions raised in the aftermath of the DigiNotar breach,628 ENISA policy documents629 and lobbying by the Dutch government630 suggests that the DigiNotar affair has made its mark in the drafting process. In April 2014, the European Parliament adopted

---

624 For up to date information, see: <https://letsencrypt.org/>
625 In June 2015, the Energy & Commerce Committee in the US House of Representatives sent a letter to the four major browser vendors asking whether technical constraints to certificate issuance by CAs would be a sensible technical and policy solution to the current weakest-link problem. Perhaps, the letter indicates a deeper Congressional investigation or a policy intervention in due course. See <http://energycommerce.house.gov/letter/letters-browsers-regarding-government-certificate-authorities>, accessed 2 September 2015.
626 The latter instrument did regulate the provision of so-called “qualified signatures”, to which DigiNotar was subject. The vast majority of CAs and certificate provision fell outside the scope of the 1999 eSignatures Directive. See sections 2.4 and 8.2.
627 See also section 2.4.
629 ENISA 2011.
substantial amendments to the Commission proposal, to be approved shortly afterwards by the EU Council (national governments of the EU). The final eIDAS Regulation was published in August 2014.631 “Certificate services for website authentication” are specifically mentioned as falling within the subject matter of the instrument in article 1(c). This section comments on the underlying values, scope, security requirements, security breach notification, and liability regime of the EU Regulation.

**Underlying values.** The EU proposal focuses on availability interests to boost trust in e-commerce, neglecting confidentiality and integrity concerns connected to the systemic HTTPS vulnerabilities already outlined. Apart from failing to observe (or even reflect on the existence of) positive privacy and communications secrecy obligations under the EU Charter of Fundamental Rights, the proposal completely ignores the Snowden disclosures, which had started to emerge one year before the legislation was adopted. As will be discussed in the case study of chapter 9, the MUSCULAR disclosure shows that HTTPS significantly raises the costs of mass dragnet surveillance and has been a primary target of intelligence agency subversion. The April 2014 EU Parliament amendments and the final text ignore these developments completely.

Furthering economic interests is connected to the value of creating a single market within the EU and finds its basis in articles that are referred to in the proposal, namely article 114 (and article 26) of the Treaty on the Functioning of the European Union (‘TFEU’). Facilitating other fundamental rights values is required by the EU Charter, but the EU Regulation lacks a coherent vision on what communications security, specifically HTTPS, as regulated under the

instrument should seek to protect. The EU proposal does not provide sufficient guidance on how to balance all associated interests.

The priority given to economic interests and the lack of a coherent vision on how to balance economic and fundamental rights values will have several concrete consequences for policy. As discussed below, the Regulation gives broad powers to the European Commission with regard to its most important themes. When formulating these delegated instances of executive power, and looking for guidance at the EU proposal, European and national institutions might feel obliged or enabled to prioritize an economic rationale over the broader interests that involve information security and fundamental rights values.

Scope. The EU proposal regulates trust service providers, including CAs. All major CAs appear to fall within both US and EU jurisdiction. A usual perceived drawback of regulatory initiatives in Internet environments is that regulation is inherently local (embedded within local legal systems, such as the EU), whereas the Internet is a global communications system. If a substantial share of the SSL market were to be controlled by CAs that fall outside EU jurisdiction, this would greatly reduce the potential impact of the EU proposal. Interestingly, this is not the case here. Section 8.4 shows that roughly 80% of the CA market is controlled by a limited number of companies. A scan of the legal documentation of these CAs tells us that all major CAs have offices within the European Union. Counter-intuitively, a large majority of the SSL market appears to fall within EU jurisdiction, making regulation in itself a

---

632 Asghari et. al. 2013.
solution to consider. Recent events in data protection have, however, also shown that if the opposite were to be the case, the EU could remedy this by extending jurisdiction. In any event, EU regulation may in itself be an effective instrument to address the observed market failures and positively influence HTTPS security globally.

Other critical stakeholders in the HTTPS ecosystem, however, such as browser vendors and website operators, remain unregulated by the EU Regulation. Recital 67 makes explicit that the HTTPS provision is “entirely voluntary” for web services. The Impact Assessment of the EU Commission proposal hinted at “an obligation for legal person’s website to include trusted information (e.g. a certificate) allowing the user to verify the authenticity of the website and the existence of the legal person” and continued to explain the advantages of such an obligation. The final text of the Regulation leaves no doubt that HTTPS provision is “entirely voluntary” for web services (recital 67). Browser vendors, or software developers for that matter, are not mentioned at all. As discussed below, the limited scope impacts the proposed security measures considerably.

Security Requirements. The EU proposal introduces new obligations for CAs to adopt security requirements. According to article 18[1], CAs need to implement:

appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

The details of the security requirements will be determined by the European Commission in an implementing act (article 19[4a]). The specific security requirements are not summed up in the Regulation. So much of the impact of the security requirements provision depends on the details. The implementing acts were not published by the time the case study was concluded. The open-ended norms of article 19[1] provide flexibility for regulators and enforcers to adapt security requirements in line with best practices. But with this flexibility at a delegated regulatory level, balancing of different interests and fundamental rights values cannot be neglected.

It cannot be expected that the security requirements will contribute significantly to a state of the art in which CAs abuse market dynamics, as mentioned in previous sections. Recital 67 mentions that the security requirements should help to ‘boosting trust, providing a better experience for the user and furthering growth in the internal market’, rather than to protect the integrity and confidentiality of HTTPS. The recital seems to imply that security requirements are there to keep up the appearance of control with users (see section 6.2.), rather than meaningfully contributing to securing HTTPS communications and the systems it relies on. As observed before, an economic rationale prevails in which availability is prioritized, rather than one concerned with the broader underlying interests of information security and fundamental rights values.

Moreover, the April 2014 Parliament amendments explicitly proposed to let “industry-led initiatives, for example the Certificate Authorities/Browser Forum)” influence the determination of these requirements (recital 67). The amendment made it into the final EU Regulation. Naming an industry group as influential in a law that seeks to address failing security practices of CAs seems to indicate large industry influence. In earlier policy documents, the Commission expressed that website authentication was too complicated to
regulate and that HTTPS should not be mandatory for website operators, because the Commission itself did not provide secure communications either.\textsuperscript{635} Also, the amendments state that CAs should be subject to “light-touch and reactive ex-post supervisory activities” and that there exists “no general obligation to supervise non-qualified service providers” (i.e., CAs offering certificates for HTTPS) in recital 36. Even if the security requirements in a failing market are brought up to a certain minimum standard through an implementing act, compliance oversight will be soft or non-existent. This hardly incentivizes the hundreds of CAs in the ecosystem to clean up their act. Combined, these amendments indicate regulatory capture, implicit politics through technology,\textsuperscript{636} or perhaps a mix of both. It does not indicate an ambition to actually secure HTTPS communications.

Looking at the value chain, rather than isolating the CAs, also brings into view that HTTPS implementation at the most popular websites on the Internet is below 25\% as of June 2015.\textsuperscript{637} All other websites send end user traffic unencrypted across the Internet. Also, out of 185,000 of the most popular websites surveyed, only 18\% follow a more or less secure implementation; just 1\% of the total surveyed offers ‘state of the art’ protection against recently well-reported vulnerabilities such as BEAST and Heartbleed.\textsuperscript{638} While incentivizing CAs to employ good security practices is important, a real challenge that is not addressed by the EU Regulation at all lies with website operators. The EU Regulation merely briefly stated that offering HTTPS is

\textsuperscript{635} European Commission, SWD(2012) 135, p. 35 & p. 87. The argumentation in the official documentation falls short in many respects. It even argues against such an obligation, because ‘not all EU organisations are securing their website’ – which obviously is an exceptionally poor argument. See Arnbak & Van Eijk 2012.

\textsuperscript{636} See section 6.4.


“entirely voluntary” (recital 67). Requiring proper implementation from website operators that do offer HTTPS has not been considered at all.

Transparency obligations. In article 19[2], the EU Regulation introduces a security breach notification regime. The Regulation states that notification needs to occur “within 24 hours” to relevant authorities if the breach “has a significant impact,” a concept that is not defined in the law. The general public is only informed when a breach harms the “public interest” (also undefined). Again, the European Commission gets to determine those details and as mentioned before, the supervision regime is light-touch or non-obligatory (recital 36). In comparison with the Commission proposal, the Parliament further weakened the regime by mandating light-touch and ex-post supervision. Again, these amendments indicate capture of the regulatory process by dominant CAs.

Aforementioned information asymmetries and CA breaches render a stricter regime for notifications defensible. It is telling that the security breach at Verisign only became public two years after the incident and through an indirect way, when Security and Exchange Commission regulations mandated companies to notify investors of intrusions since October 2011.639 Experiences with breach notification legislation in the US, moreover, suggest that notification obligations need to be complemented with punitive (e.g., sanction and liability regimes) and proactive enforcement (e.g., as part of annual reporting) to create real incentive to notify—and avoid noncompliance by less well-intentioned companies.640 Added sanctions are particularly relevant in the case of HTTPS, since reputation losses might not affect major CAs that do not risk being thrown out of root stores for non-reporting, being too big to fail.

640 Winn 2009.
Reporting not only breaches, but also the vulnerabilities that led to them, would be a major step forward, as would a scheme of responsible disclosure. Such lessons are not included in the EU proposals or considerations at all.

Unrelated to the EU proposals, browser vendor Mozilla has proposed so-called “chain of trust transparency.” As discussed earlier, one cannot assure that HTTPS communications are subject to systematic but unnoticed surveillance without transparency, but such transparency is only starting to emerge through various (research) projects such as the browser plug-in CertPatrol for Firefox. Since mid-2013, Mozilla has been requiring in its CA policy that subordinate CA certificates “either be technically constrained or be publicly disclosed and audited.” Subordinate CAs, in other words, must either be constrained to issue certificates for only a (small set of) domain name(s)—on internal networks, for example—or their chain of trust must be publicly disclosed and audited. The aim is to hold subordinate CAs to similar standards as root CAs and make a root CA accountable for all the sub-certificates it signs. Chain of trust transparency should be encouraged throughout the HTTPS ecosystem. It is a measure especially suitable for legislation, but has not been part of any regulatory or other policymaking proposal so far.

**Liability arrangements.** As already observed, liability for security breaches is disclaimed across the HTTPS ecosystem and transferred through terms and conditions to end users. The 2012 EU Commission proposal sought to address such liability dumping by imposing a strict liability regime on CAs for “any direct damage,” with CAs bearing the burden of proving that they handled the situation non-negligently. The 2014 parliament amendments and the final text reverse this burden of proof; customers and users now have to prove malicious

---

641 Soghoian & Stamm 2012.
642 Mozilla CA certificate policy, version 2.2, 14 Feb. 2013.
intent or negligence at CAs post-breath (article 13[1]). While a liability regime may incentivize CAs to augment security, the reversion of proof does exactly the opposite of what was desirable. Users can hardly determine “from the outside” why a breach has occurred, and as discussed above the security breach notification and oversight mechanisms had been watered down considerably too, hardly taking away the information asymmetries for end users discussed in section 8.2. No argumentation is available on the motives of shifting the burden of proof with CAs, but keeping it there could have established the essential incentive for CAs to augment security. The final text of the EU Regulation allows CAs to limit liability in their terms and conditions to a certain financial amount as long as they “duly inform their customers in advance of the limitations on the use of the services they provide” (article 13[2]). This should enable the assessment of financial risk and the establishment of insurance markets (recital 37).

CA liability could theoretically internalize the externalities, but the potentially wide-ranging consequences of a breach mean that they are quickly beyond the scope of an individual firm. The fact that the leading CAs are all too big to fail reduces their exposure to liability, just like it has for the banks in the financial sector. In all likelihood, such provisions will lead to liability-avoiding legal arrangements (such as putting liabilities in separate legal entities). Insurance thus seems a key tool in distributing risk and compensation. Baldwin et. al. explain this elegantly by referring to oil tankers: the potential damages of a spill can be much larger than the value of the firm transporting the oil. Such ‘shallow pockets’ cases, which are also emerging in HTTPS communications, would require compulsory insurance beyond bare liability rules to leverage the risk of a breach. Allowing CAs to limit liability therefore is an unwise

644 This is different in the case of qualified trust services, who bear the burden of proof vis-à-vis customers.
645 Baldwin et. al. 2011, p. 127.
approach by the EU lawmaker that should be corrected if the Regulation is ever updated.

Moreover, the broader functional value chain escapes unscathed from these arrangements. Liability should be matched with security requirements and distributed among all stakeholders. CAs have their share in this risk, but are mostly unaware what value a sold certificate should protect, whereas website owners know what kinds of sensitive information they are dealing with (online banking, E-Commerce, private communications, etc.). Domain owners should be incentivized to protect their assets through HTTPS offering and implementation. Browsers have their share in the security breaches too, in particular in the case of untimely trust revocation and strengthening their CA policies (as discussed below). Another aspect that would deserve attention in the context of liability is the option for CAs and other stakeholders to pass on liability to information technology producers such as software developers, who in many cases ‘are in a better position than database owners to fix problems with information security’. The Regulation failed to consider such fundamental issues; a missed opportunity to augment browsing security and the HTTPS ecosystem.

8.7. Conclusion

HTTPS has become a de facto standard for securing web communications, but continues to be exposed to the same systemic vulnerabilities that the DigiNotar incident brought to the fore in September 2011. Four years on, the status quo hasn’t changed. The ‘weakest-link’ and ‘too big to fail’ problems still present fundamental flaws in HTTPS communications and the market for HTTPS is dominated by a few CAs that have little economic incentive to make amends to

646 Winn 2009, p.33.
the current situation. Most website operators still don’t choose to offer HTTPS to their users, or implement the protocol poorly. The liability of security incidents is still dumped on end users. The systemic vulnerabilities actually benefit rather than hurt these dominant market stakeholders.

For all its flaws, HTTPS remains a critical cybersecurity technology, as the confidentiality and integrity of web browsing cannot be assured without it. Even if HTTPS doesn’t protect communications metadata, no deployment of HTTPS means communications traverse global networks in clear text, unencrypted, unprotected. HTTPS is the practical manifestation of communications security as an objectified first line of defense. HTTPS deserves close scrutiny by the EU legislature.

In terms of solutions, technical changes to the HTTPS protocol are promising to overcome the systemic vulnerabilities of HTTPS, but face serious adoption constraints. From a regulatory perspective, the EU lawmaker missed the unique opportunity to augment the security of HTTPS when debating and finally adopting a flawed eIDAS Regulation. Overall, the Regulation does not address systemic vulnerabilities and persistent market failures, but rather exacerbates them. The legislative debate shows elements of an implicit politics in technology policymaking as well as successful lobbying from the same industry that the Regulation in its initial proposal sought to regulate.

Serious analysis of market dynamics or the positive fundamental rights obligations to secure communications have not been part of the legislative debate at all, and should have informed the policymaking surrounding the eIDAS Regulation. In addition, the eIDAS Regulation should have provided normative guidance on the balancing of confidentiality, integrity and availability of HTTPS. One of the key objectives of legislation in this space should be to ensure the enjoyment of fundamental rights such as privacy and
communications freedom and to protect users browsing the Internet against arbitrary interferences. Also, specific regulatory measures could have addressed the market failures and systemic vulnerabilities throughout the functional value chain. Security requirements should have been paired with proportionate liability provisions. Furthermore, meaningful security breach notifications and vulnerability reporting should have been coupled with proactive enforcement and meaningful sanctions in case of non-compliance. Auditing and oversight should include forensic research in addition to the existing paper audits that have proven unable to prevent the serious breaches over the last years. To this end, the scope of any legal response to augment HTTPS should include all relevant stakeholders in the functional value chain, especially web browsers and website operators.

The EU lawmaker has not even made a start in taking such consideration into account and seems far from meaningfully protecting private communications security in the networked environment. Instead of improving the security incentives in the HTTPS market, the eIDAS Regulation and its interplay with other policy cycles creates new long-term institutional dependencies on the actors whose roles should be limited from a communications security perspective. The eIDAS is set to exacerbate the surveillance and market failures in HTTPS communications.
9. The Snowden Files – Communications Security in the ‘Cloud’

Fast and secure networked communications have enabled a paradigm shift in computing in recent years. Users, corporations, governments and other organizations alike are moving their communications into remote computing farms, popularly referred to as the ‘cloud’. With the ‘Internet of things’ hitting mainstream, home appliances, wearables and cars are also connecting and committing their bits and ‘things’ to the ‘cloud’ too. The ‘cloud’ seemingly computes at your fingertips, but communications and data processing usually occur at far distance, rather than on a local computer, smartphone or device. As such, the transition into the ‘cloud’ can have serious implications for the informational autonomy and communications security of end users; governments, companies and citizens alike. Behind a veil of sanitized marketing material and interaction design, the ‘cloud’ obscures a deep dependence of users on their ‘cloud’ providers.

The ‘cloud’ business has been booming for years. Meanwhile, national security and law enforcement agencies are enjoying the ride into the ‘cloud’ too. Before Snowden’s disclosures, claims that massive communications breaches for intelligence purposes were occurring could be substantiated merely by pointing at legal and technical possibilities, a number of earlier

647 This case study is a synthesis of three earlier papers: Van Hoboken, Arnbak & Van Eijk 2012; Van Hoboken, Arnbak & Van Eijk 2013; Arnbak & Goldberg 2015. Large portions of the text are identical to the text in these papers, but this is the first instance in which these are integrated into one case study. The research and writing for the former two papers was concluded in September 2012 and May 2013 respectively. The research for Arnbak & Goldberg 2015 was concluded in September 2014. The research has been slightly updated in December 2014 and the peer-review process that lasted through to May 2015. Views and errors in the case study remain the sole responsibility of the author.


leaks, conceptual observations, as well as circumstantial evidence. Now, the string of disclosures on intelligence activities has provided detailed evidence. As Laura Poitras, one of the journalists closely working with the documents, has stated: “My vision hasn’t really changed, but what I’m able to see has vastly increased.”

When Edward Snowden revealed the PRISM surveillance operation conducted by the NSA, major US ‘cloud’ providers were directly implicated. The structural denial of a public-private surveillance partnership between the ‘cloud’ industry and governments was never that credible, but the sheer scale and sophistication has caught nearly everyone by surprise. Somewhat later, operation TEMPORA was revealed, detailing bulk intercepts by the GCHQ of submarine fiber-optic communications cables, storing all content for 3 days and communications metadata for 30 days. And in October 2013, the MUSCULAR disclosures showed how the NSA and GCHQ exploited unprotected ‘cloud’ communications by intercepting them while traversing between Google and Yahoo! datacenters, grabbing roughly 180 million communications records monthly. Many disclosures have followed since, such as MUSCULAR’s umbrella program WINDSTOP that intercepts billions of intercepted records per month.

Outside the tech policy bubble, the publication of Hollywood’s private parts and intimate moments across the Internet have made the consequences of remote computing tangible for the average user. A string of security breaches

---

652 Van Hoboken, Arnbak & Van Eijk 2012 point to several sources that had already made informed estimates about the scale of intelligence surveillance.
654 See section 9.2.
surrounding Apple’s iCloud — popularly referred to as ‘Celebgate’ or ‘The Fappening’ — received sustained and world-wide media coverage for nearly a month. Together, the incidents make clear that ‘cloud’ providers can have entirely different communications security goals than their users. Moreover, failing to protect technical security in the ‘cloud’ can have severe and rather dirty consequences.

This case study will not repeat or exhaustively examine communications security issues associated with the migration into the ‘cloud’, but focuses on one set of communications security issues. How should the EU protect private communications security in ‘cloud’ communications, as implicated in operation MUSCULAR?

Out of all the Snowden files, operation MUSCULAR is the focal point of the case study. MUSCULAR purposefully circumvented the HTTPS protections put in place by the ‘cloud’ operations of Google and Yahoo! to directly capture communications content and metadata, unbeknownst to the ‘cloud’ providers themselves. As such, in addition to the HTTPS case study of the previous chapter, the MUSCULAR case provides a perfect window into investigating the functional value chain of cloud communications. Google and Yahoo! users, meanwhile, have been fully exposed to surveillance of contact lists, photos, videos, e-mails, and calendars on a massive scale. Also, MUSCULAR enables deeper analysis of the surveillance incentives, whereas the HTTPS case focused on market dynamics for communications security.

This case study does not directly deal with government access to stored data, as enabled through operation PRISM.655 As such, transnational data transfers, the Safe Harbor regime and localization as a jurisdictional requirement under

---

655 For analysis and recommendations on the transnational aspects of government access to cloud data, see Hoboken, Arnbak & Van Eijk 2012 & 2013.
CJEU Digital Rights Ireland fall outside the scope of this case study. The case study will only discuss broader issues around transnational surveillance, data protection and lawful access as they relate operation MUSCULAR. The case study does point out, however, that lawful access can be circumvented by powerful adversaries if even a small part of the entire functional value chain of ‘cloud’ communications is insufficiently protected. Incidents in the commercial sphere, such as the ones suffered by iCloud users, are not further examined in the case study.

In terms of methodology, the case study combines descriptive, internal legal analysis with threat-modeling from computer science. In addition to reaching inter-disciplinary conclusions, the case study aims to offer academics a new analytical framework to conduct similar research. The methodology should be particularly helpful for conducting research on the interdependency of the laws and technologies for network surveillance and conducting evaluations of surveillance law as part of policymaking.

9.1. Intra- and Interdomain ‘Cloud’ Communications Value Chains

The ‘cloud’ being more of a metaphor of computing than a specific ICT or protocol, NIST has had some difficulty defining ‘cloud computing’. The first part of its definition reads:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.656

656 NIST definition of ‘cloud computing’, SP800-145, p. 6.
The second part of the NIST definition illustrates that there is not one ‘cloud’, but many different models and use cases. NIST pinpoints five essential characteristics: on-demand self-service; broad network access; resource pooling; rapid elasticity, and measured service. NIST also identifies three service models and four deployment models. The three service models are: Software as a Service (SaaS); Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The four deployment models in the NIST definition are: Private cloud, Community cloud, Public cloud and Hybrid cloud. From the NIST definition alone, twelve different deployment models of cloud computing can be distinguished. Each of these instances may have specific providers and customers, leading to varying value chains and security goals. ‘Cloud’ communications implicated in the MUSCULAR disclosures can mostly be characterized as public clouds under the Software as a Service (‘SaaS’) model, meaning cloud services providing applications and infrastructure for uses such as webmail, social networking, hosting or data storage that any end user on the web can sign up to.

The data flows in the cloud deployment models in the MUSCULAR disclosures have been partly explained and visualized by the Washington Post visualization below. The data flow between the ‘1. public Internet’ and ‘2. Front-end servers’ through the web browser has been extensively discussed in the HTTPS case study of chapter 8. This case study examines the communications security issues beyond those web-facing communications, within the private network of one ‘cloud’ provider and between the networks of cloud providers. These two communications functions are called intradomain and interdomain communications respectively.

---

657 NIST definition of “cloud computing”, SP800-145, p. 6.
In the figure, *intradomain* communications occur between ‘2. Front-end servers’, ‘3. Google’s private cloud’ and ‘4. Google’s global infrastructure’; in other words, a network owned by a single organization, whether or not it is physically located in multiple datacenters. The networks of large ‘cloud’ providers such as Google and Yahoo! will interconnect with other parts of their respective private networks (and with other networks, discussed below) at so-called “Internet exchanges”. These large hubs of Internet connectivity concentrate large numbers of ‘cloud’ and Internet service providers in order to benefit from network effects. Other stakeholders involved in ‘cloud’ communications and possibly implicated in operation MUSCULAR include service providers that lease fiber-optic communications cables or related infrastructure (such as the “cable landing stations” mentioned in the visualization), which can collectively be grouped under “fiber intermediaries”.
1. **Public Internet**
   Internet and mobile users who send Gmail, create Google Drive Documents or use other Google products over the public Internet typically do so via encrypted Web connections with Google.

2. **Front-end servers**
   All Google requests are received by front-end servers that handle and process Web requests and return the data to the user.

3. **Google’s private cloud**
   Google’s data centers, located around the world, are networks of computers linked by private fiber-optic cables. Google’s servers, located in enormous buildings under 24-hour guard, synchronize their data and work together to balance traffic loads.

4. **Google’s global infrastructure**
   Cloud companies, such as Google and Yahoo, store multiple copies of user data across geographically distributed data centers in order to improve reliability and performance. Google and Yahoo generally connect their data centers over privately owned or leased fiber-optic cables, which do not share traffic with other Internet users and companies, to enable the fastest connections and keep information secure. Until recently, these internal data networks were not encrypted. Google announced in September, however, that it is moving quickly to encrypt those connections. Yahoo’s data center links are not encrypted.

*Note: This diagram depicts data flow, not actual fiber links.*
In *interdomain* communications, traffic traverses networks belonging to different ‘cloud’ communications providers. Interdomain communications are mediated by one of the Internet’s basic communications protocols, the Border Gateway Protocol (‘BGP’). BGP enables communication between networks – called Autonomous Systems (‘ASes’) – owned by different organizations; for example, the communications between Google’s and Yahoo!’s network. ASes are interconnected, creating a graph where nodes are ASes and edges are the links between them, sometimes collectively referred to as the ‘Internet backbone’.

In interdomain communications, ASes use BGP to learn paths through the AS-level graph: an AS discovers a path to a destination AS via BGP messages received from each of its neighboring ASes. An AS then uses its local routing policies to choose a single most-preferred path to the destination AS from the set of paths it learned from its neighbors. The AS then forwards all traffic for the destination AS to the neighboring AS that announced the most-preferred path. Importantly, the local policies used to determine route selection are often based on the price of forwarding traffic to the neighboring AS that announced the path, as well as on the number of ASes on the path announced by that neighbor. Available bandwidth and possible network congestion are key in this regard, not physical distance. This means that it can sometimes be cheaper to forward traffic through a neighboring AS that is physically located far away. This situation is common, for example, in South America, where

---

660 See Arnbak & Goldberg 2015 for more extensive elaboration.
661 Caesar & Rexford 2005, p. 5-6.
662 This is where the business model of Content Delivery Networks (‘CDNs’), such as Akamai, comes in. Akamai is both a CDN and an AS. Leading CDNs have a massive number of connections, and as such a single CDN might have a single AS number but then physically be connected in many locations all over the world. A user at home accessing a website hosted by Akamai would do interdomain communications, probably going from the AS of his or her ISP directly to Akamai’s AS. Paths to ASes tend to be very short (2 hops) because CDNs are so well connected.
network paths between two South American endpoint ASes often cross undersea cables to Miami. As such, interdomain ‘cloud’ communications may travel all over the world and pass many different communications networks and infrastructure, even if computing seemingly occurs at the fingertip of the end user.

The Functional Value Chain

The ‘cloud’ communications settings implicated in operation MUSCULAR include roughly five stakeholders: i) the end user; ii) his ‘cloud’ provider; iii) Internet exchanges; iv) fiber intermediaries, and v) a third party ‘cloud’ provider in the case of interdomain communications.

End users. The ‘cloud’ deployments implicated in MUSCULAR combine a SaaS model in a public cloud. Here, ‘cloud’ communications providers offer services that end users can easily sign up to – or are forced into by means of coupling the service provision with an operating system or device – but cannot exert control over with regard to the functionality of the service on offer. Sometimes, end users get to control some aspects of data processing, such as visibility controls or a ‘do not track’-option. But when it comes to communications security protection, users usually completely depend on their ‘cloud’ provider.

A vital point that emerges from the functional value chain in both intradomain and interdomain communications is the invisibility of these communications to the end user and public at large. The end-point of any given ‘cloud’ communication is not at the frond-end server of a provider, as a whole world

---

663 Madory 2013.
664 IXmaps, see <http://ixmaps.ca>.
rife with vulnerabilities lies behind the visible front-end of the ‘cloud’. The data protection issues emerging from the migration into the cloud had been cause for alarm in both the research and policy communities for some time, but communications security issues that might arise in both intradomain and interdomain ‘cloud’ communications only caused alarm among the general public after the operation MUSCULAR was disclosed, and perhaps even more when a string of breaches around Apple’s iCloud hit the mainstream news.

‘Cloud’ providers operate and manage huge swaths of communications and data behind the front-end server end users interact with. Both in intradomain and interdomain ‘cloud’ communications settings, companies like Yahoo! and Google replicate data across multiple servers that periodically send data to each other, for backup and synchronization purposes. These servers are located in different areas to prevent valuable data from being lost in case of outages or errors in one location:

“Rather than storing each user’s data on a single machine or set of machines, we distribute all data—including our own—across many computers in different locations. We then chunk and replicate the data over multiple systems to avoid a single point of failure.”

Communications and data in the ‘cloud’ are thus always on the move in the interest of availability. Amazon, another major ‘cloud’ provider, uses similar techniques and encourages end users and customers to use multiple datacenters for reasons of availability.

---

665 Google, Data and Security, see <http://www.google.com/about/datacenters/inside/data-security/index.html>, accessed 2 September 2015; Google, Data Center Locations, see <http://www.google.com/about/datacenters/inside/locations/index.html>, accessed 2 September 2015 (Google datacenter locations are distributed worldwide); See also Yingying Chen et al., A First Look at Inter-Data Center Traffic Characteristics via Yahoo! Datasets, IEEE INFOCOM 2011, see <http://www-users.cs.umn.edu/~yingying/papers/infocom11-yingying-paper.pdf>, accessed 2 September 2015 (Yahoo datacenter locations).

Amazon operates state-of-the-art, highly-available data centers. Although rare, failures can occur that affect the availability of instances that are in the same location. If you host all your instances in a single location that is affected by such a failure, none of your instances would be available.

In interdomain communications settings, communications travel between ‘cloud’ providers. Communications on the internet backbone are deliberately not encrypted by default through the BGP protocol in the interest of availability, thus creating many paths for communications to one end-point. The economic and availability interests underlying day-to-day routing make interdomain ‘cloud’ communications inherently insecure. The emerging underlying values of the BGP add to the general claim that basic Internet protocols were not designed with communications security in mind; instead, its design reflects a focus on providing robust and reliable communications while minimizing cost.

Of course, ‘cloud’ providers may decide to implement specific communications security measures when connecting their respective users to each other’s networks. In e-mail, for example, a protocol called STARTTLS can signal between cloud providers, say Gmail and Hotmail, that encryption is offered – similar to HTTPS in web browsing. Several other protocols enable encrypted communications through voice calling, instant messaging and other communications uses. As discussed in section 9.4, it is hardly possible for end users to figure out what protection ‘cloud’ providers have on offer; even after a range of incidents including the Snowden files.
Moreover, encryption itself is no complete panacea for communications security. Encryption can help combat some of the specific communications risks connected to cloud computing and the MUSCULAR operation, but even communications that are encrypted end-to-end expose ‘metadata’ (e.g., who is communicating, the length of the communication, timing information, etc.). Metadata is extremely useful for both bulk and targeted surveillance, as it can be used to reconstruct surprisingly detailed information about the ‘social graph’ (network of contacts) of the communicants and even the ‘contents’ of the network traffic.667 The gist of this technical literature is that even encryption cannot hide the fact that a user made a certain telephone call or visited the server hosting a particular site. For example, one might learn from the “metadata” that someone calls his psychotherapist four times on Christmas day, or that an Internet user visited the server hosting the site www.hivmedicineinfo.com; this “metadata” immediately leaks information about diseases that the user might be likely to have, even if the actual contents of the communications were encrypted. The EU Data Retention Directive was precisely aimed at mass metadata collection, rather than the contents of communications.

The integration by cloud providers of other roles and stakeholders in ‘cloud’ communications value chains is another crucial development for communications security. Increasingly, major ‘cloud’ providers are not only offering (web-based) ‘cloud’ communications and connected services, but moving into the business of offering the soft- and hardware at the endpoints of ‘cloud’ communications too. Companies such as Apple, Google and Amazon all try to integrate the end-points of their respective ‘clouds’ into the functional value chain of their services. Google, for example, produces smartphones,

667 For an extensive body of technical literature on the subject of using ‘metadata’ to reconstruct information about the ‘contents’ of encrypted network traffic, see Brad Miller et. al. 2014, p. 146-164.
operating systems, apps and other hard- and software that force end users into signing up for their ‘cloud’ offerings across the ‘cloud’ communications value chain. This integration of hardware, software and service provision has important implications for the market and surveillance dynamics in the ‘cloud’ communications value chain, and ultimately end user communications security.

*Internet exchanges, fiber intermediaries* and other *Internet service providers* (such as the end users’ telecommunications, Internet access provider or Wi-Fi access point) constitute stakeholders as both intradomain and interdomain ‘cloud’ communications pass through their networks. All of these stakeholders present potential points in the functional value chain in which ‘cloud’ communications security can be breached, even if communications remain in the *intradomain*, within the logical boundaries of the internal networks of one ‘cloud’ provider. This became clear through the string of Snowden disclosures, discussed in the next section.

### 9.2. Incidents and Systemic Vulnerabilities

This section discusses a number of incidents in cloud communications. It covers intradomain communications, the Internet backbone, interdomain communications and hardware. Then it extrapolates these incidents to formulate several systemic vulnerabilities in ‘cloud’ communications.

In *intradomain* communications, the revealed MUSCULAR/TURMOIL program illustrates how the NSA exploited the technical infrastructure of the ‘cloud’ to acquire traffic between Google and Yahoo! servers, collecting up to 180 million user records per month. MUSCULAR impacted all types of users throughout the Google and Yahoo! customer base, including Internet users, corporations, institutions and governments. As discussed in the previous
section, organizations such as Yahoo! and Google replicate data across multiple servers that periodically send data to each other, likely for the purpose of backup and synchronization. These servers are located in diverse locations, likely to prevent valuable data from being lost in case of outages, or errors, in one location. Whereas the communications between users and cloud providers may have been secured through HTTPS, the traffic sent between these ‘cloud’ servers was unencrypted.

With the news report, the Washington Post published one original slide that indicates that the program was explicitly founded to intercept communications in the weakest point of the functional ‘cloud’ communications value chain. MUSCULAR targeted ‘cloud’ communications beyond the web-facing (and HTTPS encrypted) communications path, exactly at the point where the encryption was removed from the ‘cloud’.

---

Beyond the Google Front End server, where SSL-encryption is “added and removed”, the NSA slide shows how traffic traverses the Google ‘cloud’ in clear text. Gmail, Google Docs and Maps are mentioned in the drawing. So beyond the public Internet, MUSCULAR intercepts ‘cloud’ communications directly from the Google cloud. The Washington Post story did not reveal exactly how MUSCULAR operated, and where exactly the interception takes place as the ‘cloud’ communications flow between Google’s datacenters. The newspaper offered several possible scenarios alongside MUSCULAR’s disclosure.669

How the NSA’s spying on Google’s internal network is intercepting data on Americans

The NSA intercepts user account information as it flows between data centers. The precise collection points and methods are unknown. These are among the possibilities:

**SCENARIO 1**
Two data centers in separate geographic locations — wholly owned and operated by Google — are connected by Google-owned fiber, or by cables and network equipment managed and leased from a third party.

**SCENARIO 2**
Google owns and operates major internet connections, including some undersea cables, making them a primary Internet provider.

**SCENARIO 3**
Google also leases private links from global internet providers that manage the network and its equipment, such as an internet exchange.

**SCENARIO 4**
Other times, Google’s servers are housed in shared hosting facilities with other companies.

**How the NSA May Spy on Google**

- **Cable landing station**
  The point at which an undersea cable makes landfall and its links are routed to land-based networks.

- **Internet exchange**
  A device that channels incoming data and directs data toward its intended destination.

- **Shared data center**

The NSA may have figured out ways to tap directly into Google's privately owned and managed internet links. The NSA's British counterpart, the GCHQ, may have induced or compelled a third party — such as the operator of a cable landing station, a major internet exchange or a data center that Google shares with other companies — to install surveillance equipment on Google's private cables.
Along with these technical weaknesses, MUSCULAR exploited loopholes in US surveillance law to enable mass surveillance of these intradomain communications. International communications intercepted on US soil are regulated by FISA and overseen by Congress and the FISA Court. By contrast, international communications, when collected abroad, are regulated by the permissive legal regime of Executive Order 12333, solely governed and primarily overseen by the executive branch. An operation can be regulated under EO 12333 if it is designed to adhere to two main criteria: 1) it does not “intentionally target a US person” (e.g., bulk surveillance) and 2) it is conducted abroad. EO 12333 and its underlying guidelines (notably, USSID 18) contain permissive presumptions of foreignness, and as long as users are not intentionally targeted, operations on foreign soil are presumed to affect foreigners exclusively. Since foreigners do not enjoy the legal protections provided by the Fourth Amendment, conducting operations abroad under EO 12333 enables the intelligence community to circumvent constitutional and statutory safeguards in the Patriot Act and FISA, even when Americans’ data are intercepted. Many NSA programs, also those discussed below, are based on EO 12333, adopted in 1981 by the Reagan Administration and not substantially updated since. According to the NSA, EO 12333 is the “primary legal authority” for its operations.

More generally, the Internet backbone is an important target of sustained communications breaches, both in the intradomain and interdomain ‘cloud’ communications settings. A vast number of disclosures indicate that the NSA has many capabilities to collect Internet traffic on a large scale soil by tapping into transnational fiber-optic cables through which ‘cloud’ communications

670 Arnbak & Goldberg 2015.
A single transnational fiber-optic cable can aggregate huge volumes of both interdomain and intradomain telecommunications (including Internet, telephony, fax, and VoIP traffic) generated by hundreds of different ASes. Many of these operations resort under a division of the NSA known as Special Sources Operation.

One program, codenamed WINDSTOP, deals with collection from so-called “second party” countries (the United States, the United Kingdom, Canada, New Zealand, Australia). The MUSCULAR program (discussed before) falls under the umbrella of WINDSTOP, as does the INCENSER program, which likely collects billions of records each month. INCENSER involves tapping into the network linking one trans-Atlantic fiber-optic cable from the United States to the United Kingdom (the “FLAG Atlantic 1” cable) to another transnational cable from the United Kingdom to Japan via the Mediterranean, India, and China (the “FLAG Europe Asia” cable). The cable was tapped on British soil by the British Government Communications Headquarters (GCHQ), and the collected traffic was shared with the NSA. Moreover, the NSA’s RAMPART-A operation is a cable-tapping program undertaken in collaboration with a foreign “third-party” country, i.e., a country other than one of the “five eye” countries. The foreign country taps into international fiber-
optic cables located on its own territory, moves the raw traffic to a processing center on its territory that contains NSA-provided equipment, and forwards the traffic to a NSA site on US soil. The three largest RAMPART sites—codenamed AZUREPHOENIX, SPINNERET, and MOONLIGHTPATH—tap a total of seventy different international cables. Although the locations of various sites remain unknown, media reports suggest that both Germany and Denmark are involved.\textsuperscript{678} According to journalists with access to the source material, many similar programs exist, implicating a wide range of Western governments.\textsuperscript{679}

In interdomain communications, where traffic traverses networks belonging to different organizations, weaknesses in the design of routing protocols and hardware can be deliberately exploited to intercept traffic. Manipulations of the BGP protocol can cause network traffic to take unusual paths.\textsuperscript{680} In 2013, global Internet monitoring and research company Renesys observed a number of highly-targeted manipulations of BGP that caused traffic sent between two American endpoint ASes to be routed through Iceland.\textsuperscript{681} On August 2, 2013, manipulator AS Siminn in Iceland used BGP to send an “impersonated route” for an IP address block, allowing Siminn to intercept traffic sent between two endpoints in Denver, Colorado.\textsuperscript{682} A summary of that manipulation is shown in the figure below.\textsuperscript{683}

\textsuperscript{678} Geist et al. 2014.
\textsuperscript{679} Gellman & DeLong 2013. The Washington Post has also revealed some aspects of a similar program called INCENSER (of which the technical details remain unknown), that apparently collected 14 billion user records in the same 30 day period.
\textsuperscript{680} Arnbak & Goldberg 2015, section II.3.B.1, extensively describes the technical underpinnings of deliberate BGP manipulations for surveillance purposes. Section II.3.B.1. describes manipulations of the Domain Name System (DNS) protocol in detail. These are not included here in the case study.
\textsuperscript{681} See Peterson 2013.
\textsuperscript{682} Cowie 2013
\textsuperscript{683} Taken from Arnbak & Goldberg 2015.
On June 31, 2013, manipulator AS Siminn in Iceland used BGP to send an “impersonated route” for IP address block 206.51.69.0/24, allowing Siminn to intercept traffic sent between two endpoints in Denver, CO, USA.

Traffic, originating at an endpoint physically located in Denver and logically located inside Atrato’s AS, travels to an Icelandic AS (Siminn) and then back to its destination (physically located in Denver and logically located in Qwest/Centurylink’s AS). Sending a BGP message that “impersonates” a legitimate destination AS means that the manipulator AS (Icelandic AS Siminn) sends a BGP message that claims a false route to the IP address block (206.51.69.0/24). As shown in the figure above, the manipulator AS (Siminn) falsely claims that the IP address block 206.51.69.0/24 is allocated to Siminn’s own customer AS, the Icelandic Opin Kerfi AS 48685. In reality, that IP address block is allocated to the legitimate destination AS (Qwest/Centurylink). Because BGP lacks mechanisms that can authenticate allocations of IP address blocks, the
manipulator’s neighbors will accept this impersonated route, and forward all traffic destined to the IP addresses in the disputed block to the manipulator’s AS\(^685\) (Siminn) instead of the legitimate destination (Qwest/Centurylink).

Renesys also observed an AS based in Belarus performing similar BGP manipulations.\(^686\) Similar incidents have occurred periodically across the Internet.\(^687\) In 2010, for example, a routing incident caused traffic sent between multiple American endpoint ASes to be diverted through China Telecom during a single eighteen-minute time period.\(^688\) In 2008, a presentation at DEFCON demonstrated how these manipulations could be performed in a covert manner.\(^689\) This method could be used to confound the network measurement mechanisms\(^690\) that researchers used to detect the 2010 and 2013 incidents mentioned above.

In terms of ‘cloud’ communications hardware, several Snowden disclosures involve one particularly interesting class of manipulations: hacking into routers or switches. Recent disclosures suggest that the NSA has the capability to take control of remote routers and intercept communications in transit. The HEADWATER, SCHOOLMONTANA, SIERRAMONTANA, and STUCCOMONTANA programs are examples of this capability at work.\(^691\) The NSA can also physically tamper with US-made routers for surveillance purposes.\(^692\) Another possibly relevant class of manipulations is the

\(^{685}\) Cowie 2013. For a comprehensive view of BGP security, see Goldberg 2014.
\(^{686}\) Cowie 2013.
\(^{687}\) Butler et. al, 2010.
\(^{688}\) Cowie 2013.
\(^{689}\) Kapela & Pilosov 2008.
\(^{690}\) Typically, researchers identify BGP manipulations using diagnostic tools like traceroute (Malkin 1993) or BGP looking glasses such as D. Meyer, University of Oregon Route Views Archive Project, at <http://www.routeviews.org>, accessed 2 September 2015. However, a clever and dedicated adversary can use various techniques to avoid detection by these diagnostic tools, as demonstrated by Kapela & Pilosov 2008.
\(^{691}\) Appelbaum et. al. 2013; See also Storm 2014.
\(^{692}\) Greenwald 2014.
SECONDATE program, which the NSA calls “an exploitation technique that takes advantage of web-based protocols and man-in-the-middle capabilities,” designed for “mass exploitation of traffic passing through network choke points as well as surgical target selection”. All these techniques could be used to intercept ‘cloud’ communications, both in the intra- and interdomain.

The extent to which the described incidents and capabilities are used by intelligence agencies is unknown. National security secrecy – not so much on the operational level but at the policy level – still limits exhaustive independent analysis and evaluation. But the recently increased transparency does offer sufficient basis to observe that many technical possibilities exist to breach the security of ‘cloud’ communications.

Systemic Vulnerabilities

Based on the described incidents, this study can identify several systemic vulnerabilities of intradomain and interdomain ‘cloud’ communications. First, persistent information asymmetries exist between ‘cloud’ providers and their users. It is striking how little the general public could be aware of the vulnerabilities of ‘cloud communications’, and the extent to which their communications were exposed. Before the MUSCULAR disclosure, little to nothing could be inferred from public policy documents or ‘cloud’ offerings themselves. Information asymmetries are abundant in the cloud communications, and disable informed consumer decisions about communications security. Snowden’s disclosures have shed some light on the systemic vulnerabilities in ‘cloud’ communications, but it is hard or even

693 Gallagher & Greenwald 2014.
694 Only in response, NGO’s have started campaigns to increase such transparency. For instance NGO EFF at <https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what>, accessed 2 September 2015
impossible to evaluate different ‘cloud’ offerings based on the communications security practices on offer.

Second, endogenous incentives for communications security seem absent in the cloud industry. Pre-Snowden, major weaknesses in communications security existed at established ‘cloud’ farms with consistent multi-billion dollar revenues and startups alike. Only after Snowden’s disclosures are some ‘cloud’ providers starting to make amends to augment communications security. Some of them were quick to react when operation MUSCULAR became public; Google pledged and implemented apparently robust encryption in the intradomain communications setting in a matter of weeks. Many other market leaders, however, still do not offer basic communications security protection.695 This points at perverse incentives to provide ‘cloud’ communications security. These dynamics are further discussed in section 9.3.

Third, the incidents described show that vulnerabilities will be readily exploited in practice for the purpose of surveillance. A large number of both passive (“learning or using information”, such as operation TEMPORA) and active cyberattacks (“altering system resources or operation”, such as protocol manipulations and soft- and hardware hacking) have now been observed in the real world. The hypothetical undertone of widely used terms in communications security systems design and policy – such as “risk” and “threat” – seems to obscure a reality in which theoretical weaknesses are widely exploited in practice. Statements to the contrary, made before Snowden’s disclosures, are either incomplete or untrustworthy.696 The attack

---

landscape in the space of government surveillance presents, to cite Microsoft press release in the wake of the MUSCULAR disclosures, an “advanced persistent threat” to communications security, “alongside sophisticated malware”.697

Fourth, attackers seek out the weakest point in the functional value chain. As soon as one point in the value chain had apparently been secured and presented legal or technical constraints on surveillance, vulnerabilities in other parts of the value chain were exploited. Exploring new weaknesses along the functional value chain has been an ongoing process. In the 1990s, conventional telecommunications providers across the world were required by law to set up their networks to facilitate lawful access to data and wiretapping.698 When webmail and social network providers started to offer HTTPS encryption on web-facing front-end servers, communications interception in transit with conventional telecommunications providers became less effective. Therefore, governments increasingly directed surveillance efforts towards ‘cloud’ providers that offer services ‘on top of’ Internet access provision.699 The MUSCULAR operation explicitly targets points in the functional value chain beyond ‘cloud’ front-end servers, where the TLS/SSL encryption is stripped from the ‘cloud’ communications path, and moves into the intra- and interdomain area. Also, these communications were not requested directly from the ‘cloud’ providers through government access requests such as, for example, operation PRISM, which requires warrants from the FISA Court for access to ‘cloud’ data. Rather, an interdependent legal and technical infrastructure was designed to enable access to those huge volumes of data to which access was legally and technically constrained, or in any case made too time-consuming.

698 Already in 2005, the usefulness of traditional wiretapping schemes was declining due to the rise of IP-based (packet-switched) communications. See TILT & Dialogic 2005.
This implies that as long as interdependent technical and legal loopholes exist to breach ‘cloud’ communications security at other points in the functional value chain, these will be considered and may eventually may be exploited. As such, meaningful communications security can only exist end-to-end, along the entire functional value chain.

Fifth, attackers seek out attack surfaces under the lowest relatively weak legal protection. One prominent legal loophole featuring across the Snowden files is the fact that non-US persons do not enjoy the protections of the Fourth Amendment of the US Constitution. Only US citizens do.\(^\text{700}\) Indeed, the MUSCULAR program illustrates how the NSA could assume authority under a weaker legal regime – i.e. Executive Order 12333 rather than the Patriot Act or the Foreign Intelligence Surveillance Act – to acquire ‘cloud’ communications by targeting Google and Yahoo! datacenters located on foreign territory.\(^\text{701}\) By conducting the operation abroad, in close cooperation with British counterpart GCHQ, the operation did not need court approval by the Foreign Intelligence Surveillance Court. Foreigners do not enjoy constitutional protection and, in this case, US citizens can even be monitored under low legal protection as long as an intelligence agency can construct plausible presumptions that surveillance does not “intentionally target” a US person and when the surveillance is conducted abroad, the permissive legal regime under EO 12333 applies. Under EO 12333, operations from abroad can be presumed to affect foreigners rather than US citizens.

---

\(^{700}\) The principle was first established by the US Supreme Court in \textit{United States v. Verdugo-Urquidez}, 494 US 259, 261 (1990). The case concerned a warrantless search of a Mexican citizen’s house, in Mexico, suspected of drug trafficking. The principle was recently confirmed in \textit{Clapper v. Amnesty International USA a.o.}, 133 S.Ct. 1138, 1154 (2013). The case was brought by several civil society groups, claiming the unconstitutionality of warrantless bulk surveillance of their international communications.

\(^{701}\) Gellman & Soltani 2013.
In response to the Snowden disclosures, the US Government seemingly seeks to restore the trust of foreigners in US cloud offerings. Presidential Policy Directive 28 purportedly aims at providing some added level of protection for foreigners against intelligence gathering operations conducted by the US intelligence community.\textsuperscript{702} The stated ambitions, however, have not yet resulted in meaningful added protection. In the realm of lawful access for law enforcement purposes, US Congress has recently adopted a law that extends the protections afforded to US citizens under the 1974 Privacy Act to citizens of certain foreign countries, to be determined by the Dept. of Justice. The extension would provide a means for citizens of indicated foreign countries to start legal proceedings in the US.\textsuperscript{703} However, many law enforcement uses are exempted from the 1974 Privacy Act. Providing these trust signals does indicate a desire to make amends to the lack of legal protection of foreigners in US clouds, but at this point it is still hard to discern or robustly analyze the effects of these recent efforts.\textsuperscript{704}

In addition to eavesdropping on intradomain traffic, such loopholes also exist in the interdomain setting. Interdomain routing with Border Gateway Protocol (BGP) can naturally cause traffic originating in a US network to be routed abroad, even when it is destined for an endpoint located within a country. Additionally, core Internet protocols—BGP and the Domain Name System (DNS)—can be deliberately manipulated to force traffic originating in American networks to be routed abroad.\textsuperscript{705} These deliberate manipulations can fall within the permissive EO 12333 regime and can be used to collect, in bulk, all Internet traffic (including metadata and content) sent between a pair of

\textsuperscript{705} Arnbak & Goldberg 2015.
networks, even if both networks are located within one country. For these reasons, the legal incentives to conduct surveillance under EO 12333 are substantial. These loopholes have not only been exploited by the NSA. In later disclosures, such as operation RAMPART-A, it has become clear that European intelligence agencies cooperate closely with the NSA, to enable surveillance on their respective citizens.

*The NSA documents state that under RAMPART-A, foreign partners “provide access to cables and host US equipment.” This allows the agency to covertly tap into “congestion points around the world” where it says it can intercept the content of phone calls, faxes, e-mails, internet chats, data from virtual private networks, and calls made using Voice over IP software like Skype.*

Based on the same disclosure, Snowden made a statement to the European Parliament that the close cooperation between the US and fifteen European countries serves to provide a “European bazaar” in terms of access to networked communications through bilateral cooperation.

Taken together, along the functional value chain many interdependent technical and legal loopholes exist for attackers to exploit ‘cloud’ communications.

### 9.3. Incentives

In chapter 6, the study already made clear that beyond well-known legal justifications of intelligence gathering, such as counter-terrorism, a wide range of dynamics are at play that feed into the powerful incentives for government

---

surveillance. In fact, the Snowden Files show that intelligence agencies across the globe seem keen on acquiring as many communications as possible and express grandiose desires such as: “collect it all, sniff it all, know it all”\(^7\) to serve a broad range of interests. Along with these general observations, this section takes a deeper look at the underlying surveillance (and to a lesser extent, market) incentives for intelligence gathering operations such as MUSCULAR. Why was MUSCULAR conducted, and why do the glaring vulnerabilities in functional ‘cloud’ communications value chain exist in the first place? Understanding the incentives and broader dynamics at play is critical in assessing the c.i.a.-triad in ‘cloud’ communications (section 9.4) and the role for technology (section 9.5) as well as the EU lawmaker (section 9.6) in improving end user communications security protection (section 9.7).

**Surveillance incentives**

**Changing economics of intelligence gathering.** The economics of surveillance are rapidly changing, as advances in technology make communications breaches, datamining and relatively cheap.\(^7\) As discussed in section 4.6., these socio-technical developments have fundamentally changed the cost-benefit equation of surveillance. Whereas financial, physical and technological constraints may have barred intelligence agencies from breaching communications security by default in the past, today the economics of surveillance are such that intelligence agencies have decided to collect everything and then analyze what communications are valuable to retain, rather than the age-old adage of ‘select before you collect’. This may explain why the NSA has been building a massive new analysis center to collect all information.


\(^7\) On the “changing economics of surveillance”, see Soghoian 2009, p. 384-387. See also Bankston & Soltani 2013.
relevant to US interests. And why the Chief Technology Officer of the CIA stated (for recruiting purposes) that “it is nearly within our grasp to compute on all human generated information”, with the aim of “protecting and advancing America’s interests.” Add to that the fact that end users are massively migrating their communications to the cloud, and one understands why the NSA has declared today’s networked environment and age a “golden age of signals intelligence.”

**Quid pro quo.** A 2009 report by the Dutch Review Committee on the Intelligence and Security Services (‘CTIVD’) offers some insight into the cooperation between, and data collection and sharing practices of intelligence agencies internationally. The report interestingly observes that day to day data sharing between agencies is “mediated” by the principle of ‘quid pro quo’: what you give is what you get. The reasoning is that by giving away intelligence to foreign intelligence agencies, and getting some in return, intelligence agencies serve national security interests. There is a clear interest for intelligence agencies to increase their own levels of access to information in the private sector and to have as broad as possible legal powers. Interestingly, these practices are described in market terms, while privacy, confidentiality and information security interests of public and private actors are not at all mentioned. As such, the exchange between governmental agencies in

---

713 Idem, p.12.
714 Idem, p. 12-16. The risk of giving away too much information and in doing so limiting the ability of the Dutch intelligence agency for future intelligence sharing, is also recognized. The
different countries seems to introduce a dynamic of its own: it is perceived as a means to establish a superior information position over other agencies. In addition, these dynamics are explicitly used among allied intelligence agencies to grant counterparts a read-in or a proverbial place at the table when new programs or activities are discussed.

**Circumvention domestic legal safeguards internationally.** Allied intelligence agencies seem to have limited incentives to protect their citizens against surveillance, as it has become clear that agencies assist each other in circumventing legal safeguards at home by conducting surveillance on each other’s citizens and sharing the information bilaterally. One could even posit wonder whether agencies actually rely on the capacity of foreign agencies to breach communications security at home. Even ever-dominant US intelligence agencies seem to spy on US persons with the help of European intelligence agencies in order to avoid constitutional restrictions in the US. The MUSCULAR disclosures made clear that the NSA-run program is operated in close cooperation with its British counterpart GCHQ and an unknown British telecommunications provider. The Echelon program, uncovered in the months before 9/11, has been seen by many as a way to circumvent national constitutional restrictions. The RAMPART-A program, briefly discussed in section 9.2, makes use of similar methods to circumvent legal safeguards.

---

CITVD critiques the short term ‘ad hoc’ drive of Dutch intelligence analysts and advises a more strategic vision on longer term interests to Dutch national security.

716 This mirrors what Swire has described as an increasing dependency of agencies that have no access to cloud data (‘the have-nots’) on those that have (‘the haves’). Swire 2012, p. 1.


If no meaningful restrictions are placed on the exchange of foreign intelligence between agencies, it is likely that communications security breaches take place at a geographical and/or technical point in the functional value chain where communications security practices and legal safeguards are the lowest. Such practices seriously endanger information security and confidentiality interests of cloud customers and causes a race to the bottom in terms of communications security interests.

**Market incentives**

*Information asymmetry and negative externalities.* ‘Cloud’ providers compete heavily on communications availability, but apart from statements that such providers are deeply committed to communications privacy and security, end users are hardly able to assess how ‘cloud’ providers perform on confidentiality and integrity assurances. This asymmetry in the information position of end users is a serious risk in itself, and stands in the way of careful decision-making about the use of cloud services, even if broad surveillance of ‘cloud’ communications is not a core concern for a specific end user. The risk may be structural risk, since it is not in the interest of cloud providers to remove this asymmetry. In the end, the harms of breached communications are first and foremost suffered by end users, not their providers. Only when breaches are publicized may these negative externalities be internalized by companies going forward. The major Silicon Valley ‘cloud’ farms implicated in operation MUSCULAR, as well as in the iCloud breaches, had not secured intra- and interdomain ‘cloud’ communications before suffering reputational damages post-breach.

Wiretapping in the intra- and interdomain might not even have been part of the threat models of ‘cloud’ providers and even Internet exchanges. One senior systems engineer of the Amsterdam Internet Exchange, one of the largest of its
kind globally, declared at a hearing in the Dutch Parliament shortly after the first Snowden disclosures that even a large, professional organization like AMS-IX did not consider intelligence agencies in its communications security threat models. The theoretical possibility of vulnerabilities in the functional value chain apparently did not create sufficient incentive across the market to implement communications security measures along the functional value chain to counter arbitrary fundamental rights infringements. Finally, cloud providers may not be in a position to provide an answer in good faith on these complex issues, let alone any guarantees, if they fall under national security gag orders or if their services depend on other ‘cloud’ providers. With regard to operation MUSCULAR, the intelligence community has even resorted to hacking into the privately owned infrastructure of cloud providers. The information asymmetries thus extend to the relationship between government and industry. A cloud provider can hardly provide assurances of communications security to the market if its intra- and interdomain communications are the subject of systematic cyberattacks by intelligence agencies.

Changing incentives post-Snowden? Strikingly, in response to the global outcry after the MUSCULAR disclosures, several major cloud companies announced or even implemented considerable communications security measures in a matter of weeks. Google and Yahoo! have moved to encrypt the

---

720 Soghoian 2009.
721 This is the case in particular for cloud providers that only offer software as a service and use the infrastructure of third parties for the storage and processing of cloud data; so-called SaaS providers (Software as a Service), as opposed to IaaS (Infrastructure as a Service). Google and Yahoo!, implicated in operation MUSCULAR, offer a hybrid model of SaaS, IaaS for certain elements and PaaS (Platform as a Service), but also face challenges as their service depend on other providers (internet exchanges and fiber intermediaries) and their relationship with intelligence agencies may fall under a gag order.
intradomain communication links between their data centers, and a number of other corporations have followed suit.  

Apparently, the lack of communications security protection was not so much due to technological complexity, but lacking economic incentives: the year after the first Snowden disclosures saw a significant halt in the booming prospects of US cloud providers. Concerns of governmental and corporate customers have spurred market developments such as federated and encrypted solutions as well as ‘national clouds’ that are ‘Patriot Act Proof’ – whatever the merits of these claims in practice. Several European governments announced projects for localized clouds for the same reason.  

Responding to a strong desire for users to know what kind of protection they can count on, NGOs are starting to shine some light on how ‘cloud’ offerings compete on communications security, for example EFF’s ‘Who Has Your Back’, ‘Secure Messaging Scorecard’ and ‘Encrypt the Web Report’ projects. The ‘Encrypt the Web Report’, last updated November 2014, ranks US ‘cloud’ offerings in the following infographic:

---

722 EFF 2014.
726 EFF 2014.
727 See <https://www.eff.org/secure-messaging-scorecard>, accessed 2 September 2015.
<table>
<thead>
<tr>
<th>Company</th>
<th>Encrypts data center links</th>
<th>Supports HTTPS (Strict)</th>
<th>HTTPS Strict (HSTS)</th>
<th>Forward Secrecy</th>
<th>STARTTLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>Undetermined</td>
<td>Limited</td>
<td>X</td>
<td>Undetermined</td>
<td>X</td>
</tr>
<tr>
<td>Apple</td>
<td>Undetermined</td>
<td>(Close)</td>
<td>X</td>
<td>Undetermined</td>
<td>(mac.com, itouch.com)</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>Undetermined</td>
<td>Undetermined</td>
<td>X</td>
<td>Undetermined</td>
<td>(art.net)</td>
</tr>
<tr>
<td>Comcast</td>
<td>Undetermined</td>
<td>Undetermined</td>
<td>X</td>
<td>Undetermined</td>
<td>(comcast.net)</td>
</tr>
<tr>
<td>Dropbox</td>
<td>In progress</td>
<td>In progress</td>
<td>In progress</td>
<td>In progress</td>
<td>In progress (facebook.com)</td>
</tr>
<tr>
<td>Facebook</td>
<td>Undetermined</td>
<td></td>
<td>Undetermined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Foursquare</td>
<td>Undetermined</td>
<td></td>
<td>Undetermined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google</td>
<td></td>
<td></td>
<td>In progress</td>
<td>In progress</td>
<td>In progress</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>Contemplating</td>
<td>Planned 2014</td>
<td>Planned 2014</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>In progress</td>
<td>Planned 2014</td>
<td>Outlook.com</td>
<td></td>
<td>(outlook.com)</td>
</tr>
<tr>
<td>Myspace</td>
<td>Undetermined</td>
<td>X</td>
<td>X</td>
<td>Undetermined</td>
<td>X</td>
</tr>
<tr>
<td>Sonic.net</td>
<td></td>
<td>In progress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twitter</td>
<td></td>
<td>In progress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tumblr</td>
<td></td>
<td>Planned 2014</td>
<td>Planned 2014</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Verizon</td>
<td>Undetermined</td>
<td>Undetermined</td>
<td>X</td>
<td>Undetermined</td>
<td>(verizon.net)</td>
</tr>
<tr>
<td>Yahoo</td>
<td></td>
<td>Default for Mail planned 2014</td>
<td>Planned 2014</td>
<td>Yahoo.com</td>
<td>X</td>
</tr>
</tbody>
</table>

Notes: The information in this chart comes from several sources: the companies who responded to our survey questions; the information we have determined by independently examining the listed websites and services, and published reports. Some of the surveyed companies did not respond to the survey.

Recognizing that some of these steps will take time to implement, we gave credit to companies that either (1) have implemented or (2) have concrete plans to implement the listed encryption process, as needed.

For STARTTLS, the red and grey shading indicates whether or not the company is a major email service provider. While we encourage all companies to implement STARTTLS, even if they only provide email for their own employees, the issue is most critical for companies that provide email communications to the public.

Google implements HSTS on accounts.google.com for all browsers that support HSTS, which at the time of this writing are Chrome, Chromium, Firefox, Opera, and Safari. HSTS on other Google domains is only functional in Chrome, Chromium, and Safari.
Based on the infographic, a general observation can be made: even after Snowden’s disclosures, to which the “Encrypt the Web Report” responds, leading US cloud farms such as Amazon and Apple fail to offer basic communications security protection for end-users. Beyond the implementation of HTTPS that encrypts the communications paths between users and front-end servers, the picture is very mixed indeed. On the other side of the scale, since the summer of 2015 Twitter maintains a real-time online dataset that reports which e-mail providers offer STARTTLS when Twitter sends e-mail notifications to users. At the start of its reporting in August 2015, Twitter reports an impressive 94% of global e-mail traffic is encrypted using STARTTLS.729 The numbers Google report are somewhat less impressive: 80% for outgoing e-mail and 63% for incoming e-mail, percentages that have stabilized in the last years.730 Still, across the board the ‘cloud’ market scores quite poorly on encrypting intradomain communications links between datacenters.

Will ‘cloud’ communications externalities be internalized going forward? While some providers have changed communications security policies across their ‘cloud’ offerings, incentives to provide basic communications security protection still seem to be lacking throughout the entire ‘cloud’ market, even post-Snowden. Moreover, the infographic merely lists US ‘cloud’ providers that have received much of the attention after Snowden’s disclosures. How lesser-known ‘cloud’ providers and providers from other countries would rank in the infographic is completely unknown. But even if the vast majority of providers decides to secure some parts of the functional value chain for ‘cloud’ communications, critical gaps in the protection of private communications

remain. As the next section will show, and extensively discussed in chapter 4, fundamental rights mandate a more strict role for the EU lawmaker in protecting private communications security regardless of ‘actor’ or sensitivity of ‘personal data’ involved.

9.4. The c.i.a.-Triad in Cloud Communications

As operation MUSCULAR and the rest of the Snowden disclosures show, and many scholars and security experts have argued before them,\footnote{Van Hoboken, Arnbak & Van Eijk 2013 and the overview of scholars listed across the publication.} the intelligence community across the world has exploited the new relationship between the security attributes in the ‘cloud’ c.i.a.-triad on an unprecedented scale. As such, the transition of computing from local hard- and software into the ‘cloud’ profoundly changes end user confidentiality, integrity and availability interests.

With regard to confidentiality, the mere possibility that communications security in the cloud may be breached for surveillance purposes has an obvious impact on communications confidentiality itself and related interests of end user autonomy, control and intellectual freedom. Before the MUSCULAR disclosures, end users were mostly unaware of the risks of entrusting sensitive communications and data to ‘cloud’ providers. Even in the current climate, end users can never be sure exactly how cloud providers secure their communications and cannot inform themselves whether or not cloud providers cooperate closely with government entities when it comes to intelligence gathering.\footnote{In the 2012 EPIC v. NSA case concerning the cooperation between Google and the NSA, the The District Court Virginia ruled that neither Google nor the NSA needed to confirm or deny whether they cooperate. See EPIC v. NSA, 11-5233 (6th Circuit 2012).} End users also lack insight into the activities of the business partners of ‘cloud’ providers (such as back-up providers, fiber intermediaries and Internet exchanges), into actual removal of communicated data from the
servers of cloud providers (and their business partners), into the actual security of the new range of devices provided by ‘cloud’ providers and into what happens with ‘cloud’ communications and data in the event of bankruptcy, a takeover or if they wish to end their relationship or agreement with a provider. True confidentiality in the cloud is therefore hard to achieve. ‘Cloud’ markets and current legal obligations for transparency and security requirements thus fail to protect confidentiality interests.

The exact confidentiality interests at stake depend on several factors. Some communications are highly sensitive due to the insight they can provide into the private life of one person, others help to map or gain insight into political movements, corporations or even entire populations. Such sensitive communications extend far beyond the data that are considered ‘personal’; for example research data sets, drafts of news articles, as well as state and trade secrets. The impact on confidentiality interests also depends on the cloud user concerned. Most organizations responsible for the confidentiality concerns of their customers or citizens face substantial confidentiality concerns when deciding to entrust communications to cloud computing, in particular when end users rely on their storage and processing policies – as is the case in usual Software as a Service (SaaS) public clouds implicated in operation MUSCULAR.

Companies and government agencies that seek to safeguard their strategic interests, intellectual property and related business or government secrets may actually want to cooperate with the same intelligence agencies that breach

---

733 Including, but not limited to: identity and biometric data, medical data, financial data, electronic communication data, data from and about politicians, journalists, government officials, political and religious groups and data about the whereabouts and mobility patterns of the population.
communications security in the ‘cloud’, and deem this in their self-interest.\textsuperscript{734} The NSA and many other intelligence agencies combine the tasks of defending communications security at home and breaching it abroad.\textsuperscript{735} In the ensuing public-private partnership, customer confidentiality interests may be left out of the equation. Close relationships between cloud providers and a particular intelligence agency can be problematic, not only with regard to data of citizens, but in business-to-business and business-to-government relationships too. The merits of the claims of the European cloud industry aggressively promoting ‘Patriot Act proof’ or ‘domestic’ cloud offerings notwithstanding,\textsuperscript{736} customers that are forced to share the processing or control of their communications and data with their cloud provider should be in a better position to evaluate and trust the security of their communications vis-à-vis their provider, domestic and foreign governments as well as cybercriminals and other threats and vulnerabilities.

At first glance,\textit{ integrity} may seem less of a concern in non-webfacing ‘cloud’ communications. However, the MUSCULAR, TEMPORA and other disclosures have illuminated a wide range of potential and realized man-in-the-middle attacks that exploit lacking integrity assurances in the intra- and interdomain of ‘cloud’ communications. The cyber-arsenal of intelligence agencies in non-webfacing ‘clouds’ seems vast, and includes protocol manipulations, coercing Internet exchanges and fiber intermediaries into cooperation and hacking into networked communications infrastructure. Beyond confidentiality, such measures may breach communications integrity as in the current set-up of many ‘cloud’ communications users can hardly be

\begin{flushleft}
\textsuperscript{734} The Dutch General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) is actively offering assistance to such organizations. See <https://www.aivd.nl/onderwerpen-0/cyber-security/taak-aivd/>, accessed 2 September 2015.
\textsuperscript{735} Arnbak & Goldberg 2015.
\textsuperscript{736} See section 9.3.
\end{flushleft}
assured as to who gets to modify or tamper with their communications in the functional value chain of ‘cloud’ communications.

In terms of availability, the shift of computing to remote locations – and the ‘access to a shared pool of configurable computing resources’ it implies – fully depends on the availability of ‘cloud’ communications and related communications infrastructures. Indeed, the spectacular rise of communications availability – in terms of reliable high-speed Internet connectivity and powerful end user hardware – have enabled the shift from local to ‘cloud’ computing. The ‘cloud’ is always-on, always there and always syncing. Benchmarking on availability is conducted by several companies; benchmarking provider CloudHarmony ranks ‘cloud’ availability by scanning dozens of ‘cloud’ providers in real-time and presenting the results live on its website, showing for example a 99.9985% uptime for the Amazon EC2 ‘cloud’ and a 99.9997% uptime for Google Cloud Storage. Such performance is striking by all means. If there’s one thing ‘cloud’ providers prioritize, invest in and compete on, it is availability at all times. It chimes well with NIST’s identification of the five essential characteristics for ‘cloud’ computing: on-demand self-service; broad network access; resource pooling; rapid elasticity, and measured service. Therefore, the focus of protection afforded through legislation should focus on the confidentiality and integrity interests that the market itself provides to a much lesser extent.

Whether or not the risk of communications security breaches is high, actual harm of communications breaches through surveillance is traditionally hard to quantify, even after the Snowden disclosures. The stakes can be high: breached communications may lead to compromised authentication credentials for

---

737 See NIST ‘cloud computing’ definition, cited in section 9.1.
739 See NIST ‘cloud computing’ definition, cited in section 9.1.
financial accounts, trade secrets, impersonation online, exposure to ransomware and reputation damages. But the actual damages remain hard to get a figure on. This complicates the development of insurance markets and the substantiation of liability suits.

More tangible risks – visible to end users – relate to access to services, the availability of communications and whether cloud providers actually remove communications and data upon deletion by the customer. Such tangible risks and benefits may get prioritized by low-end or even mid-end security customers, even if these cloud customers won’t be able to know what happens to their communications, who has access to them and how often. So in practice, the risk of a confidentiality or integrity breach in non-webfacing ‘cloud’ communications is one concern in a long list of quantifiable risks related to communications security. When data confidentiality is found vital, the situation has led to calls for regulatory action and termination of cloud contracts – such as in cases of medical data storage in electronic patient record systems and biometric data processing in relation to passports.740 These developments all point towards strict fundamental rights protection.

A Fundamental Rights Perspective on ‘Cloud’ Communications741

Several court proceedings that respond to operation MUSCULAR are on the horizon to establish the fundamental rights perspective on ‘cloud’

740 For a discussion, see Whittacker 2012.
741 Falling outside the scope of this case study, Van Hoboken, Arnbak & Van Eijk 2013 also analyzed cloud surveillance from an international law perspective. Transnational surveillance has an impact on foreign territory but the requests for access, and communications security breaches for that matter, could take place on the territory of the country claiming transnational intelligence jurisdiction. While the intrusion by law enforcement or intelligence agencies into computers on foreign territory would entail the extraterritorial use of power, transnational surveillance through internationally operating cloud or communications services – or bilateral cooperation to that end as in the RAMPART-A program discussed in section 9.2. and 9.3. – may not be an infringement of international law.
communications before European courts. Applying the analytical framework of chapter 4 to the ‘cloud’, it seems likely that the EU lawmaker has positive obligations – a system responsibility – to protect end user ‘cloud’ communications in the intra- and interdomain. All elements of the ‘fair balance’ test of the ECtHR and the analytical framework of *CJEU Digital Rights Ireland* point in the direction of positive obligations for lawmakers to secure ‘cloud’ communications comprehensively.

**Essence.** First, the essence of article 8 ECtHR is impaired, as operation MUSCULAR intercepted metadata, content, address books, pictures, video and a wide range of other data from ‘cloud’ providers without their cooperation. Procedural legal safeguards were thus circumvented; in fact, the absence of communications security measures created the incentives for the abuse of these highly sensitive communications. The lack of communications security safeguards enabled mass surveillance. In a broader sense, the Snowden disclosures show that any unencrypted communication runs a serious risk of interception and being fully analyzed in bulk. The fact that operation MUSCULAR was just one in a series of operations resorting under overarching umbrella programs indicates that MUSCULAR was no incident, but part of a structural effort to breach ‘cloud’ communications in bulk.

Moreover, the essence of rights seems particularly at risk in operation MUSCULAR. The number of individuals affected, across the globe and user base, the invasiveness of the breach and its duration all support the observation that the exploitation of the lack of communications security offered in the ‘cloud’ is particularly serious and warrants “laws specifically adopted to ensure full confidentiality and integrity” as demanded by *CJEU Digital Rights Ireland* in the case of the blanket retention of metadata. Not having such laws in place, or having such laws but allowing economic considerations to dictate whether a “particularly high level” of communications security is afforded to end users, is
likely in breach of the EU Charter. As the essence seems particularly at risk, European courts may be more inclined to adopt substantial safeguards, along with procedural ones. To that effect, along with transparency obligations and effective oversight, detailed substantial security requirements – such as requiring full end-to-end encryption – are defensible. Such requirements need to cover the entire functional value chain of ‘cloud’ communications to provide effective, practical protection of the fundamental rights at stake.

The full picture of technical solutions – discussed in section 9.5 – may be considered in this regard to meet fundamental rights obligations. Limiting the scope to one actor, to ‘personal data’ or to one specific measure such as HTTPS will be insufficient, as the full functional value chain of ‘cloud’ communications should be addressed at once. Maintaining weakest links along the functional value chain of ‘cloud’ communications is enough for mass surveillance to occur and protections to be rendered – in the words of the ECtHR – “theoretical and illusory, rather than practical and effective”.

The conceptualization of communications security as an ‘objectified’ first line of defense is helpful is this regard: without end-to-end encryption of all ‘cloud’ communications, countless opportunities remain for extensive man-in-the-middle attacks in today’s dominant communications environment. Communications that are routed across the Internet backbone are exposed to countless vulnerabilities and threats: Internet exchanges, fiber intermediaries, routing hardware are just some of the weak points in the functional value chain implicated in the Snowden Files that relate to the ‘cloud’.

At the same time, end users must enjoy protection against arbitrary interferences with their fundamental rights. To realize such protection,

---

encryption can make a start to protect important aspects of these communications and serve as an objectified first line of defense against mass surveillance. Meaningful communications security can only exist end-to-end, and in full realization that “end-to-end” must include the entire functional value chain, and not stop at the front-end server of a ‘cloud’ company; HTTPS deployment was the very reason for operation MUSCULAR to exist in the first place.

**Complexity.** Second, legislating ‘cloud’ communications security seems not particularly complex. In terms of legislative complexity, even if the lawmaker has a lot of ground to cover, the lacking market incentives and insufficiently advanced threat models can no longer be an excuse to leave this vital communications setting exposed to unfettered surveillance. For lawmakers, legislating communications security in the ‘cloud’ seems not so much an issue of complexity but one of elevating best practices – observed for example in EFF’s ‘Encrypt the Web Report’ discussed in section 9.3 – to legal standards across ‘cloud’ markets. In terms of technological complexity, Google secured its intra- and interdomain ‘cloud’ communications paths relatively quickly after operation MUSCULAR was disclosed. Several ‘cloud’ farms have now announced and proposed significant communications security measures.

**Consensus.** Third, the E-Privacy Directive may count as a European consensus on the normative force of protecting end user communications security. The E-Privacy Directive contains a general obligation for conventional telecommunications providers to respect and guarantee confidential communications and to secure personal data. In its most recent update, the communications security provisions were substantially strengthened. A new update of the E-Privacy Directive was announced by the new European Commission in its Digital Single Market Communication, and communications
security has in itself seen substantial legislative action over the last years across
the five policy cycles of EU communications security law.

In the data protection policy cycle, the Article 29 Working Party already
established that “communications between cloud provider and client as well as
between data centers should be encrypted” in 2012. As we will see in the
next section, ‘cloud’ providers seem to be included within the scope of the
currently debated new NIS Directive and its security obligations. In its
‘Snowden Report’ of March 2014, the European Parliament adopted a
resolution calling for “rerouting of Internet traffic or full end-to-end encryption
of all Internet traffic so as to avoid the current risks associated with
unnecessary routing of traffic through the territory of countries that do not meet
basic standards on fundamental rights, data protection and privacy.” In
addition, the Internet Architecture Board has issued a statement in November
2014 on Internet confidentiality, indicating that “protocol designers,
developers, and operators [should] make encryption the norm for Internet
traffic.”

Collision other legitimate interests. Fourth, the question arises whether a
positive obligation to secure ‘cloud’ communications will collide with other
fundamental rights. General agreement seems to exist that rather than collide,
communications security in the ‘cloud’ would support fundamental rights such
as privacy, freedom of expression, the freedom of thought and opinion.

744 European Parliament resolution of 12 March 2014 on the US NSA surveillance programme,
surveillance bodies in various Member States and their impact on EU citizens’ fundamental
rights and on transatlantic cooperation in Justice and Home Affairs, A7-0139/2014, para. 106.
745 Internet Architecture Board, Statement on Internet Confidentiality, 14 Nov. 2014, at
September 2015.
MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10b7a2>, accessed 2 September
2015.
Usually, policy debates are successfully framed by law enforcement agencies that claim that robust communications security complicates surveillance, which strikes against legitimate societal interests such as law enforcement and national security. The question arises whether this is true in the case of ‘cloud’ communications per se, and public SaaS-clouds implicated in operation MUSCULAR in particular.

Rather than through hacking, fundamental rights compliant surveillance must occur in the ‘cloud’ through legal process; ‘in accordance with law’ is one of the primary requirements of government surveillance under article 8 ECHR. MUSCULAR was designed to circumvent legal process. If ‘cloud’ communications were to be fully encrypted, surveillance would still be possible by requesting the data directly at these providers under legal regimes that correspond with the requirements crystallized through decades of case-law in fundamental rights law. An assessment of lawful request requirements is not part of this case study, but it is essential to realize that providing secure ‘cloud’ communications need not stand in the way of legitimate surveillance. The appropriate maxim in this regard seems to be to secure communications end-to-end, leaving no other possibility of intercepting these communications outside the realm of lawful access; falling squarely in the realm of checks and balances on power in free, democratic societies. In the ‘cloud’, communications security can create the essential leverage between secretive bulk surveillance that circumvents legal safeguards and legitimate targeted surveillance, while protecting end users against a myriad of illegitimate attackers. Communications security does not have to obstruct lawful access; moreover, as in ECtHR *M.K. v. France*, affording robust communications (or ‘data’) security does not take away the fundamental rights evaluation and the urgency of the debate on the proper balance between surveillance, privacy and communications freedom.
Recently, the relationship between lawful access and communications security has been the subject of extensive debate. An essential element in the negotiation between communications security and surveillance is the trade-off between a robust communications infrastructure for everyone or one that is deliberately weakened for the benefit of all attackers, legitimate and illegitimate alike.\textsuperscript{747} As soon as communications are weakened to enable certain forms of mass or direct surveillance, or data collection directly by public authorities rather than indirectly through lawful access, everyone can exploit those weaknesses – such as backdoors.

In response to the recently resurrected “crypto wars” of the 1990s, a group of leading computer security experts names similar arguments, along with forcefully arguing against deliberate backdoors in networked communications because it strikes against “forward secrecy” best practices, increasing complexity and thus vulnerabilities and because backdoors provide concentrated targets to attackers willing to exploit these “golden keys” to a wealth of networked communications.\textsuperscript{748} The group also questions the vague

\textsuperscript{747} Schneier 2014.
\textsuperscript{748} Abelson et. al. 2015, p.2 In similar vain, see Zittrain at \textless https://medium.com/message/dear-prime-minister-cameron-20th-century-solutions-wont-help-21st-century-surveillance-f12d7a3d300\textgreater , accessed 2 September 2015. Another poignant criticism to deliberately weakening of communications infrastructure comes from writer Cory Doctorow, who with a touch of sarcasm provides a practical perspective on the merits of proposals of U.K Prime Minister David Cameron: “This, then, is what David Cameron is proposing: All Britons’ communications must be easy for criminals, voyeurs and foreign spies to intercept; Any firms within reach of the UK government must be banned from producing secure software; All major code repositories, such as Github and Sourceforge, must be blocked; Search engines must not answer queries about web-pages that carry secure software; All major academic security work in the UK must cease -- security research must only take place in proprietary research environments where there is no onus to publish one's findings, such as industry R&D and the security services; All packets in and out of the country, and within the country, must be subject to Chinese-style deep-packet inspection and any packets that appear to originate from secure software must be dropped; Existing walled gardens (like iOS and games consoles) must be ordered to ban their users from installing secure software; Anyone visiting the country from abroad must have their smartphones held at the border until they leave; Proprietary operating system vendors (Microsoft and Apple) must be ordered to redesign their operating systems as walled gardens that only allow users to run software from an app store, which will not sell or give secure software to Britons; Free/open source operating systems -- that power the energy, banking, ecommerce, and infrastructure sectors -- must be banned outright.” See
nature of the ‘backdoor’ proposals and formulates 25 questions that it argues need to be addressed, for the policy debate on the matter to be technically well-informed.249

A far less frequently occurring conundrum is the question of mandatory key disclosure to decrypt communications that were encrypted not by a ‘cloud’ provider, but a user. This case study does not discuss the legitimacy or desirability of mandatory key disclosure, but does observe that in the wide majority of cases, certainly in public SaaS-clouds that were implicated in the MUSCULAR disclosures, the provider, not the user, owns the keys and will not provide full control of keys to end users. Even the spirited debate on the encryption of new iPhones becomes somewhat less tense as soon as one realizes that Apple maintains control of the keys to the entire iCloud that processes much of the data on the device.750 Access to those iCloud data is regulated by several legal instruments that are challenged across the US legal system in the wake of Snowden’s disclosures. The encryption of iPhones, meanwhile, means that billions of end users enjoy communications and data security once their new device has gone lost.

Moreover, even if full end-to-end encryption were to be deployed across the networked communications environment that gives users exclusive control of the keys to the communications, ‘cloud’ providers can still provide various highly valuable datapoints for intelligence gathering and law enforcement purposes. Communications metadata such as location and IP-address are hardly possible to hide.751 Moreover, the Snowden Files contain numerous examples – such as the ones described in section 9.2. – of intelligence agencies

249 Abelson et. al. 2015, section 4.
751 See sections 9.1 and 9.5.
successfully accessing encrypted communications too. In sum, several forms of both mass and targeted surveillance remain possible in the ‘cloud’, especially when the cloud provider controls the keys and even if the encryption is applied by the user.

**Necessity positive obligation.** Fifth, and finally, the enjoyment of fundamental rights by end users of the ‘cloud’ remains extremely vulnerable to surveillance as long as positive obligations do not exist. Especially in a public cloud setting along SaaS-models as breached in operation MUSCULAR, a user cannot protect himself but depends on the cloud provider for the enjoyment of fundamental rights and the protection against arbitrary national security interferences.\textsuperscript{752} Even if ‘cloud’ users may want to protect themselves by applying encryption end-to-end, Google’s and Yahoo!’s public SaaS-clouds hardly allow them to, and serious usability issues, costs, and technical complications arise. In addition, key management, the impossibilities of protecting metadata such as location and the commercial incentives of ‘cloud’ providers to structurally datamine end users for targeted advertising remain serious drawbacks to the wide adoption of user controlled encryption in the ‘cloud’. In this context, to emphasize confidentiality and integrity over the availability of ‘cloud’ communications is not merely a fundamental rights requirement, especially since *CJEU Digital Rights Ireland*,\textsuperscript{753} but also resonates with the new definition of communications security adopted through consensus by the engineering community at the IETF.\textsuperscript{754}

An added argument is the spectacularly lowered costs of mass surveillance in the ‘cloud’. In earlier communications environments, normative restrictions on

\textsuperscript{752} See section 4.5. \\
\textsuperscript{753} See section 4.2. \\
\textsuperscript{754} See section 5.2.
surveillance have automatically been in place due to the nature of our communications environment and the practical, technical restrictions on surveillance it inherently possessed. An ephemeral, real-life conversation in the park remains costly and hard to intercept. But many of these conversations now take place though Internet-mediated communications, particularly the ‘cloud’. The ‘cloud’ has taken away many of the practical, technical restrictions on surveillance that historically protected users. In the ‘cloud’, new normative restrictions on surveillance must be put in place to tilt the balance of fundamental rights protection back to users.

Possible reasonable limits to positive obligations on part of the EU lawmaker seem hardly applicable in this case. A positive obligation to end-to-end encryption on part of the cloud provider does not seem a disproportionate burden on the part of the EU lawmaker. The E-Privacy Directive already contains similar language for telecommunications providers, as does the data protection cycle. These protections need to be extended beyond conventional communications and personal data contexts to include newer forms of Internet-mediated communications, such as the ‘cloud’. The fact that many ‘cloud’ providers have already stepped up their efforts since MUSCULAR was revealed, even if only Google and Yahoo! clouds were directly implicated by the disclosure, shows that these concerns are not limited to one case but are recognized across the entire industry.

Clearly, national security serves as a legitimate interest for limiting the enjoyment of a certain fundamental right in order to conduct surveillance in the ‘cloud’. But with the Snowden disclosures, it has become clear that the balance between the principle (fundamental right) and its specific limitation (national security) has gone missing. National security serves as a fruitful concept to

755 See section 9.6.
legitimize covert government surveillance in areas as diverse as economic espionage, agriculture or climate change policymaking.\textsuperscript{756} The exception seems to have become the rule.

The CoE Commissioner for Human Rights recently called for leadership of the CoE and the ECtHR to limit the scope or the current ambiguity of what can be brought under the national security limitation under the ECHR.\textsuperscript{757} As discussed in chapter 6, this will not be easy for European courts as surveillance lies at the very heart of national security policy and thus the identity and claimed sovereignty of the nation state. But even procedural legal safeguards such as ‘accordance with the law’ and ‘foreseeability’ become rather meaningless as soon as the national security limitation can be invoked at all times by intelligence agencies. The full enjoyment of fundamental rights across Europe needs the ECtHR and CJEU to provide a definition of national security.

\textbf{9.5. Technical Solutions}

The technical solutions to overcome the vulnerabilities exploited in operation MUSCULAR are well-known. In its ‘Encrypt the Web Report’ project, the Electronic Frontier Foundation maintains an updated scorecard in which leading Internet companies are rated for their adoption of encryption policies, including “Encrypts data center links,” “Supports HTTPS,” “HTTPS Strict (HSTS),” “Forward Secrecy,” and “STARTTLS.”\textsuperscript{758} These technical solutions augment end user communications security in both intra- and interdomain communications significantly. In addition, the Resource Public Key

\textsuperscript{756} As part of a new book, journalist Glenn Greenwald published several new source material, including an NSA slide (nr. 45) titled “Serving Our Customers”, that include the U.S. Department of Agriculture and Commerce. See <http://glenngreenwald.net/pdf/NoPlaceToHide-Documents-Compressed.pdf>, accessed 2 September 2015.  
\textsuperscript{758} EFF 2014.
Infrastructure (RPKI) can also help combat some of the specific risks of the systemic vulnerabilities identified. And there are new efforts underway to enable turn-key encryption of websites through the LetsEncrypt project.759

Purely technical solutions like encryption, DNSSEC, and the RPKI can help combat some of the specific security risks of cloud communications, but still are no panacea. However, although encryption can certainly thwart attempts to read the content of collected communications, as discussed under section 9.3 adoption is still in its infancy. As discussed in section 9.1, even if encrypted traffic protects the content of individual communications, the same communications still expose metadata that can be used to reconstruct surprisingly detailed information about the social graph of communicants and the contents of communications. In addition, the RPKI can limit the scope and impact of some of the protocol manipulations identified in section 9.2, but cannot completely eliminate them, and it remains far from being fully deployed today.760 And new technical loopholes will likely continue to be discovered by security researchers and the intelligence community; thus, reliance on purely technical solutions alone is not sufficient protection against the systemic vulnerabilities in ‘cloud’ communications. In sum, legislation needs to play a role in protecting users in the ‘cloud’.

9.6. Current and Proposed EU Legislation

Given the systemic vulnerabilities, perverse incentives and the fundamental rights at stake in the functional ‘cloud’ communications value chain, is the EU living up to its system responsibility of protecting ‘cloud’ communications,

760 Cooper 2013.
particularly in the intra- and interdomain? As observed in chapter 2, legislative action has been proposed, is being debated or very recently adopted across all EU policy cycles, which complicates analysis in this section. But even if legislative debates are still ongoing, the study can already observe that the legislative efforts within the EU’s general approach to communications regulation and in the more specific ‘cloud’ policies, including the ‘Cloud Communications’ of 2012 and 2014, offer little hope for improvement.

The ongoing revision of the EU data protection directive is seen by many as the proper instrument to protect end user ‘cloud’ communications security. Indeed, the Article 29 Working Group has released an opinion on the ‘cloud’, in which it states that encryption should be the norm in the industry:

_Communications between cloud provider and client as well as between data centres should be encrypted. (...) Remote administration of the cloud platform should only take place via a secure communication channel. (...) Further technical measures aiming at ensuring confidentiality include authorization mechanisms and strong authentication (e.g. two-factor authentication)._\(^761\)

The client-provider and intradomain communications paths are covered under the opinion, but as operation MUSCULAR and its aftermath showed, leading cloud companies had not implemented these measures. A wide gap existed between what the regulator had expressed to be the state of the art, and what the industry provided. The gap existed because there was no way to tell for users or enforcement agencies such as DPAs whether these measures actually were in place. In this sense, the data protection cycle did protect ‘cloud’ users to some extent in the law books but we have witnessed an industry-wide lack of compliance in data protection in practice.

---

\(^761\) Article 29 Working Party 2012, WP 196, para. 3.4.3.3, p. 15.
Nevertheless, the solutions offered in the EU data protection policy cycle are inherently limited in affording protection of end user ‘cloud’ communications security, especially in relation to operation MUSCULAR. These limitations have already been discussed in section 3.2 of this study. The most obvious drawback is that only a subset of cloud data constitute ‘personal data’. Other cloud data for which there is a confidentiality or related communications security interest – corporate and state secrets, intellectual property and other documents – are as such not covered under data protection law. Moreover, the definition of ‘personal data’ is one of the most fiercely debated aspects of the EU data protection framework. A limitation of the definition of ‘personal data’ – for example, whether or not pseudonymized data will be excluded – may further marginalize the use of the data protection as a regulatory solution to secure ‘cloud’ communications for end users – citizens, corporations and governments alike. Another inherent drawback is that the proposed Regulation excludes national security regulations from its material scope, in a similar way to the current Data Protection Directive (95/46/EC). Consequently, the Regulation does not affect intelligence agency conduct, or the exchange with other intelligence services on a ‘quid pro quo’ basis as described in section 9.3.

Even if the E-Privacy Directive of the Telecoms Package does contain general obligations to secure networked communications confidentiality, these obligations only extend to conventional telecommunications and Internet access providers. ‘Cloud’ communications fall outside the scope of the Telecoms Package. The May 2015 Digital Single Market Communication of the European Commission does envision an update of the E-Privacy Directive and speculates on extending its scope to the information society services of the E-Commerce Directive. But these discussions will only start after the

763 See section 2.3.
conclusion of the General Data Protection Regulation. 764 The eIDAS Regulation does not cover the ‘cloud’ industry and does not impose obligations for ‘website operators’ to deploy HTTPS. 765 For some time, the Network and Information Security Directive – proposed in 2013 – did include cloud companies within its scope. 766 In the summer of 2015, however, statements from the EU institutions during hearings on the future of cybersecurity policymaking made clear that neither the EU Council, Commission nor the Parliament knew if the Directive would be adopted anytime soon. 767 Moreover, the scope of the Directive has become the subject of fierce lobbying efforts by the ‘cloud’ industry to exempt itself from these requirements and the negotiations are in complete gridlock since the fall of 2014. 768 It is completely unclear if Directive will see adoption at the EU level, and in what shape.

Finally, the EC’s Communication on ‘Unleashing the Potential of Cloud Computing in Europe’ communication (‘Cloud Communication’)769 and the policy documents of the European Cloud Partnership770 hardly mention the risks of exposed intra- and interdomain ‘cloud’ communications. The 2012 Cloud Communication stated that the EC would “report on the progress on the full set of actions in this [cloud] Strategy and present further policy and legislative proposals initiatives as needed” 771 by the end of 2013. The 2014 Cloud Communications, again, hardly mentions the issues at hand. Meanwhile, the European Cloud Partnership’s Steering Group has been calling for “the

---

migration of public IT use to the cloud” and to “move cloud use into mission critical areas of business and public life, in areas such as eID, smart cities, eHealth, eEducation, research and digital content services”.

These include critical data infrastructure for which the communications confidentiality and integrity issues seem particularly problematic, such as electronic IDs. Until this day, no concrete security measures have been proposed for ‘cloud’ communications within these specific ‘cloud’ policy documents.

In sum, most of the attention of the EU lawmaker to address the confidentiality and integrity shortcomings in ‘cloud’ communications is concentrated in the data protection policy cycle. The Article 29 Working Party advised mandating encryption and authentication in the ‘cloud’ in 2012, but its opinion was hardly followed by industry until the MUSCULAR operation was disclosed. The E-Privacy Directive already contains general communications confidentiality obligations. But the inherent limitations of the current architecture of EU law on communications security come into play: the ‘cloud’ carries much more than ‘personal data’, by providers that do not fall under the ‘ancien regime’ of telecommunications policy. The open issues could be solved in the proposed NIS Directive, but negotiations between the EU institutions are in gridlock, as Member States are reluctant to coordinate at the EU level. The resulting gap in legal protection leaves Europeans exposed to intra- and interdomain communications surveillance, in a time when we migrate all of our computing en masse to the cloud. The status quo is highly questionable from a fundamental rights perspective, but current EU law leaves the perverse surveillance and market incentives largely in place.


773 See section 2.7.
9.7. Conclusion

The rapid migration of computing from local devices to global clouds has definitively changed the trajectory of securing communications and the enjoyment of fundamental rights online. Snowden’s disclosures show how unprotected ‘cloud’ communications traversing global networks are exposed to the significant risk of being captured under surveillance operations such as MUSCULAR. The client-server relationship outlined in the HTTPS study is only a tiny part of the functional value chain of ‘cloud’ communications. Securing intra- and intradomain cloud communications includes taking a stance towards other providers in the value chain too, such as fiber intermediaries or Internet exchanges that operate the Internet backbone. The post-Snowden fact of the matter is that fully trusting every intermediary to be benevolent – rather than malicious or coerced by a foreign government to cooperate in mass ‘cloud’ surveillance projects – is futile. Still, ‘cloud’ providers focus firmly on availability, rather than aiming to assure confidentiality and integrity interests of end users in secure communications.

The case study analyzed fundamental rights requirements, as well as market and surveillance incentives. It constructed positive fundamental rights obligations to secure the ‘cloud’ across the functional value chain. Meeting these positive obligations, the EU lawmaker must embark on a complete reconsideration of the current setup of EU law. The five EU policy cycles outlined in chapter 2 leave significant parts of the functional value chain exposed to mass surveillance. This is exactly what operation MUSCULAR singled out, by intercepting these communications as the HTTPS protections were stripped off. Users could not know, nor tell, if their communications were exposed in the intra- and interdomain communications paths on the Internet backbone. MUSCULAR and other programs illuminate how lawmakers must realize that for legal process and surveillance ‘in accordance with the law’ to
become a realistic goal, the security of ‘cloud’ communications needs to be robust first. As observed in section 9.2 and 9.3, communications breaches are likely to zoom in on the vulnerable parts of the value chain, and as such the status quo of EU communications security law will offer little resolve to end users that depend on it for the protection of their ‘cloud’ communications. The perverse surveillance and market incentives identified in section 9.3 are hardly taken into account in current legislative provisions and proposals, and will continue to expose the enjoyment of fundamental rights in the ‘cloud’ to arbitrary interferences.

The EU lawmaker must step up efforts to ensure the protection of users against arbitrary surveillance interferences and their enjoyment of fundamental rights in the ‘cloud’. In addition to HTTPS, security by default against a passive attacker should be offered in all communications paths – as proposed by the IETF, IAB and the Article 29 Working Party. Failure to protect communications along the entire functional value chain entails a substantial threat of surveillance, sufficient to effectuate a breach of fundamental rights under the ECHR. A conceptualization of private communications security as a constitutional first line of defense will help to illuminate this insight. Encryption by default should count as a constitutional first line of defense, as well as authentication mechanisms to ensure communications integrity.

The cloud provider exerts the largest control over user communications (particularly in SaaS-clouds implicated under MUSCULAR) and is thus best positioned to protect users against fundamental rights violations. A broad notion of ‘end-to-end’ is needed; from the user through the front-end server of a ‘cloud’ provider, all the way through the back-end servers and the Internet backbone. Since operation MUSCULAR, distinctions between data ‘at rest’ and ‘in transit’ no longer make sense when aiming to meaningfully protect
‘cloud’ communications. All ‘cloud’ communications deserve robust protection, not merely ‘personal data’ or customer-facing communications.
PART IV: SECURING PRIVATE COMMUNICATIONS

10. Summary, Analysis and Conclusions

Over the last years, several serious communications security breaches have brought awareness to policymakers and the general public that contemporary economic, social and political life critically depends on the security of the networked communications environment. At the same time, communications security is under continuous pressure from a multitude of threats. To name just a few examples, mass surveillance by Western government has become an undeniable reality, private and public sector communications security incidents dominate headlines all over the world on a daily basis, persistent market failures abound in communications security markets and critical technologies and protocols we all rely on face vulnerability after vulnerability. Amidst increasing dependence and growing concern that our private communications in the networked environment are systematically insecure, this study chose as its central research question:

how should the EU lawmaker protect private communications security?

In answering the research question, the study offered the first in-depth historical analysis in the legal literature of over three decades of EU communications security law (Part I). Subsequently, the study researched the concepts and tools for the EU lawmaker based on fundamental rights, computer science and political science perspectives (Part II). These insights have led to the development of a procedural model for EU communications security legislation, which formed the basis of two case studies on communications protocol HTTPS and ‘cloud’ communications through the lens of the Snowden disclosures, operation MUSCULAR in particular (Part III). In the following
sections, the study summarizes the findings of the previous chapters, followed by a general conclusion and recommendations for the EU lawmaker in section 10.4. The study adopts a multi-disciplinary approach, combining legal research methods with insights and original research from computer science, security economics and political science perspectives. The study is the first of its kind on the thorny conundrum of securing private communications through EU law.

10.1. Part I: A History of EU Communications Security Law

Five EU Communications Security ‘Policy Cycles’

The historical analysis of Part I described how, after a surge of legislative attention for communications security during the so-called crypto wars of the 1990s and relative calm in the years after, the EU lawmaker revamped its interest in communications security in the 2012/2013 legislative season. Since then, considerable legislative programs have been adopted or initiated, all noting the vital importance of secure communications for the functioning of contemporary society.

The study identified five EU communications security ‘policy cycles’: i) network and information security; ii) data protection; iii) the Telecoms Package; iv) digital certificates and signatures, and v) cybercrime. National security is not an explicit policy cycle of EU lawmaking, as the EU Treaties have determined that national security is the “sole competence of Member States”. Nonetheless, the historical analysis has found watershed moments across the five policy cycles in which communications security was framed – sometimes explicitly, but often implicitly or covertly – as an issue of national security; often by EU Member States, particularly the United Kingdom. But the adoption of the EU Charter of Fundamental Rights in 2009 obliges the EU
lawmaker to guarantee fundamental rights protection in the legal instruments it signs into EU law. In addition, with the explosion in networked communications use and functions across our information society, vital societal interests deserve evermore serious consideration by the EU lawmaker. National security can no longer be outright excluded from EU lawmaking, if EU law seeks to protect European citizens and IT-customers going forward.

In all of these five policy cycles, the study examined the ‘security’ definitions, scope, provisions and enforcement arrangements. Covering a time-span of roughly three decades, the historical analysis formed the basis of conceptual problems uncovered by this study, and the fundamental reconceptualization of EU communications security law the study proposes.

**Definitions.** The historical analysis shows how ‘security’ definitions are incoherent and their elements left unexplained by the lawmaker. A clear understanding of the origins of the definitions across the policy cycles is lacking, as the definitions use entirely different words to describe communications security. This has important consequences for which interests are prioritized by the EU lawmaker. In tracing back the historical roots of the early EU communications policies of the 1990s, this study found that most EU definitions for securing systems can ultimately be connected to a well-understood definition of security in computer science: protecting confidentiality, integrity and availability to authorized entities (the ‘c.i.a.-triad’). Since those early days in communications security policymaking, the lawmaker has not explicitly developed the elements of the c.i.a.-triad and failed to provide useful guidance how to balance the often competing interests of confidentiality, integrity and availability in specific communications contexts. Overall, availability is prioritized over confidentiality and integrity as legal instruments often refer to the importance of continuity of service provision in a digital economy. The evident connection of the c.i.a.-triad to fundamental
rights such as communications secrecy, privacy and communications freedom is hardly developed. As these confidentiality and integrity interests are insufficiently provided for in these five policy cycles, the EU lawmaker’s approach to legislating communications security runs serious risks of violating the EU Charter. One of the central grounds for the CJEU annulling the controversial Data Retention Directive in its Digital Rights Ireland ruling is precisely because the EU lawmaker failed to adopt specific laws to ensure full confidentiality and integrity in a clear and precise manner.

**Scope.** Communications security today is regulated in a fragmented way. The legislative instruments that contain provisions on communications security have all been adopted with other underlying rationales in mind, such as liberalizing telecommunications markets, improving data protection or addressing cybercrime. Consequently, many providers relevant to communications security are not covered under the current legal framework – the most striking example being the entire set of “information society services”, such as ‘cloud’ computing providers, that mediate much of our electronic communications today. The data breach notification provisions in the Telecoms Package, for instance, only cover conventional telecommunications and Internet access providers, and thus leave web-mail providers, social networks and apps untouched. In today’s networked communications environment, however, users heavily depend on communications security practices of the latter group. Regardless of the desirability of any specific legislative measure, such ‘actor’-based approaches make legislative programs vulnerable to becoming rapidly obsolete; innovation cycles move faster than regulatory cycles at the EU level. Another risk is the observed lobbying for ‘actor’-based exemptions, as ongoing debates in the ‘network and information security’ policy cycle show. Here, a continuous political battle is fought over whether a myriad of legal categories are included or exempted from the legislation – including “information society services”, “critical infrastructure providers”,

306
soft- and hardware manufacturers and an ambiguous new container category called “market operators”. The same developments can be observed in the other policy cycles. Add to these observations the differences in scoping approaches on the national level (that fall outside the scope of this study) and the aforementioned competence complexities of the EU lawmaker in the policy space of national security, the study finds a deep fragmentation and lack of legal certainty as to which providers are regulated under what EU communications security policies.

On scope, data protection law is different from the other policy cycles. It regulates the collection, processing and further use of ‘personal data’, rather than specific actors or sectors. Recently, the scope and enforcement structures of data protection have gradually expanded to cover emergent communications security issues deemed instrumental for protecting sensitive classes of personal data – for example enforcing industry-standards that mandate online pharmacies to offer encrypted HTTPS-communications to their customers in the Netherlands. While stretching data protection has increased communications security protection in such specific cases, relying on the data protection cycle to protect overall communication security will prove an untenable trajectory for several reasons. First, legislative debates are intensifying on narrowing the definition of ‘personal data’, including a new class of ‘pseudonomized data’ that may be afforded lower protection. Second, advances in computer science have rendered previous assumptions on data anonymization safeguards hollow. Data deemed properly anonymized in a previous technological ‘state of the art’, for instance by stripping the IP-address of a communication from a database, can today fairly easily be related to natural persons using big data analytics. Such technological innovations overturn the meaning of data anonymization as protective measure altogether. Third, the data protection policy cycle is not directly targeted at critical communications security providers and technologies, but only indirectly affects
those providers when personal data are processed. For example, online pharmacies in the Netherlands must now provide a HTTPS-communications to users of their websites, but the systemic vulnerabilities of the HTTPS protocol – extensively discussed in the case study of Part III – itself cannot be addressed through data protection policy. In other words, the security of the HTTPS protocol is not an issue of personal data governance. Overall, legislating communications security through instruments with different rationales and diverse historical legacies will continue to leave large areas of communications security unprotected, and systemic vulnerabilities unaddressed. The study concluded that current scoping approaches based on specific ‘actors’ or general ‘personal data’ does not protect end user communications security sufficiently.

**Provisions.** The study analyzed the development of relevant specific provisions across five policy cycles since the 1990s. Historically, the provisions in the cybercrime policy cycle have a theoretical basis in the doctrine of ‘deterrence’. Deterrence seeks to discourage a certain type of behavior, in the case of cybercrime through the adoption of increasingly tough criminal sanctions. Whereas cybercrime measures are outside the scope of the study, deterrence as a doctrine may have limited effect in the online world. Even the earliest cybercrime instruments noted that measures that protect users are the most effective means to secure communications, rather than those that seek to punish behavior. Nevertheless, deterrence remains a widely accepted doctrine for legislative action in the area of communications security at the EU level. The study pointed at the political dynamics of subjective security policymaking and cyber ‘securitization’ to point at the substantial influence of political framing to secure certain economic and strategic agendas, rather than the security of networked communications.
Another leading source of communications security legislation is the cross-reference to article 17 of the Data Protection Directive of 1995, which regulates the security of personal data. Sometimes, the EU lawmaker tailors additional provisions to the specific industry that is regulated. The Telecoms Package, for example, contains the E-Privacy Directive and the now invalid Data Retention Directive that both provide some general provisions on communications security. On protective provisions, the study recognizes three classes of regulatory tools in four policy cycles: i) security requirements such as art. 17 DPD; ii) transparency schemes such as breach notifications, and iii) liability arrangements. The latter two classes can especially be found in the original Commission proposals for the eIDAS Regulation and the Network and Information Security Directive.

The three classes of communications security provisions seem inspired by the relatively young, influential field of security economics. Security economics analyzes failing ICT security provisioning through classic economic theories of market failure: perverse incentives on the supply-side of the market, information asymmetry, lock-in, liability dumping and negative externalities. Security economics has proven to be a promising analytical tool in explaining why communications security often fails. Nonetheless, practical obstacles, however, hinder a widespread deployment of security economics insights in policymaking. First, empirical data is needed to comprehensively analyze these markets for communications security, but market operators are usually reluctant to provide objective data on security breaches to the general public, policy makers and researchers. Second, across the policy cycles the aforementioned three classes of provisions are not included jointly. Security requirements without transparency and sanctions or liability arrangements in case of negligence or compliance failure may not incentivize providers to comply with security requirements. The three classes of provisions are needed in concord to render regulation capable of influencing perverse market
incentives. Third, enforcement structures to perform security economics analyses or provide oversight of the requirements that may follow from communications security provisions are hardly existent, not on the national level nor the EU level, or only recently taking shape (see below).

Current provisions across the policy cycles can be characterized as vague and unspecific. In these instruments, specifying the details is often either delegated to implementing acts the European Commission has to formulate later on, to standardization or to self-regulation by industry entirely. Thus, the determination of the actual communications security provisioning escapes democratic scrutiny and may create legal uncertainty. In addition, history is littered with real world cases that illustrate the limits of standardization and self-regulation in communications security. For years, a deliberately weakened GSM-standard for purposes of national security surveillance exposed many European mobile phone users to serious security vulnerabilities. The inertia of the CA/Browser Forum in overcoming the systemic vulnerabilities of digital certificate-mediated communications that have plagued HTTPS communications – well before the infamous DigiNotar breached that led to a national standstill of HTTPS for over a week in the Netherlands – is another case in point.

The study found a striking difference between initially proposed legislation and provisions finally adopted and signed into EU law. Initial proposals often contained the three classes of provisions – security requirements, transparency schemes and liability arrangements – but the specific wording in final legislative texts did not. The study pointed at intense lobbying pressure from industry to prevent legislation affecting communications security. Moreover, in as specialized and technologically complex a field as communications security, legislative debates and amendments often escape public scrutiny.
Enforcement. Until recently, communications security has hardly been enforced in any of the policy cycles. Renewed public attention after several major breaches resulted in accelerated action from enforcement agencies. Data protection authorities have some indirect influence over communications security practices, as do national regulatory authorities (NRAs) in the Telecoms Package and digital signatures and certificate policy cycles. Meanwhile, ENISA (and national cybersecurity authorities) hardly have legal authority beyond providing advice. Ongoing debates in the network and information security policy cycle will show to what extent civil enforcement agencies at the EU level will be granted sufficient tools. Several Member States are proposing to place enforcement for ‘cybersecurity’ in the hands of military agencies at the Member State level, once again framing communications security as an issue of national security.

In sum, the conceptualizations of ‘security’ vastly differ per policy cycle. The result is a complex patchwork of conceptualizations, legal protections and enforcement mechanisms across today’s five policy cycles. When it comes to scope, legislation is more often informed by opportunistic economic and political motives and a legacies of market structuring, sector-specific regulation or personal data protection. The EU lawmaker has insufficient eye for the actual function of a communication, market dynamics and insights from security economics or fundamental rights. Another general observation is how the crypto wars of the mid 1990s still cast their shadow over today’s ‘security’ conceptualizations. Many ‘security’ measures were proposed by the European Commission over two decades ago, but haven’t been adopted because of resistance of several Member States in EU Council. Some quite sensible proposals, such as the end-to-end encryption obligation in the mid-1990s Telecoms Package, seem to have disappeared from public memory today. In a hyper connected society, allowing communications security to be framed as solely a national security issue is no longer an excuse to step away from
responsibilities to protect private communications. From a fundamental rights perspective, the EU lawmaker will have to shift its current approach to meet its positive obligations. Moreover, the EU lawmaker must step up its efforts to intervene in several persistent market failures that permeate communications security provision, as illustrated in the case studies of Part III.

Analytical Framework

The conclusions of the historical analysis warrant deeper conceptual analysis to develop more robust foundations for EU communications security law. In chapter 3, the study developed an analytical framework for Part II of the study along the lines of the following four research themes:

- Security: conceptual ambiguity;
- Scope: ‘personal data’ and ‘actors’;
- National security and EU communications security law;
- Security strategies: protection vis-à-vis deterrence.

Part II of the study explores these research themes in depth, from a fundamental rights, systems design and political perspective. Based on these findings, Part III develops a conceptualization of ‘security’ and model for legislating communications security by the EU lawmaker. The model forms the structure of the case studies in Part III on HTTPS communications and ‘cloud’ communications.

10.2. Part II: Theory and Tools for the EU Lawmaker

Fundamental Rights Perspectives

The communications security elements confidentiality, integrity and availability have enjoyed recognition as constitutional values long before the
European fundamental rights tradition started post-World War II. At least since the 18th century, communications confidentiality has been protected in constitutions across European nation states through ‘communications secrecy’. Since the adoption of the ECHR in 1953, ‘respect for correspondence’ has been explicitly covered in article 8. In its case law, the European Court on Human Rights consequently holds that the ECHR is a “living instrument which must be interpreted in the light of present day conditions” to provide “practical and effective, not theoretical and illusory” protection. This “living instrument” doctrine provides flexibility for the ECtHR to keep fundamental rights protection in line with socio-technical change. The ECtHR also observes that “increased vigilance” is needed to protect the constitutional values enshrined in the ECHR in the digital age.

The EU Charter of Fundamental Rights was adopted in 2009. Along with its right to privacy in article 7, in which the term ‘correspondence’ was replaced by the more technologically neutral term ‘communications’, the EU Charter separately recognizes a right to data protection in article 8. While the EU has primarily been an economic union over the last decades, its institutions now must adapt to a new constitutional reality in which fundamental rights play a central role as well. The ECtHR case law is part of the EU acquis, and the Charter (art. 52[3]) and CJEU hold that the meaning and scope of the EU Charter are the same as the rights laid down in the ECHR. Nonetheless, constitutional traditions of the Council of Europe and the EU differ significantly. The ECtHR can render national legislation incompatible with the ECHR, whereas (most of) the CJEU rulings must be followed up on by the EU Commission to ensure enforcement. The EU has little competence and thus hardly a tradition of CJEU rulings in the sphere of national security. With *CJEU Digital Rights Ireland*, this tradition may change going forward.
Positive Obligations to Legislate Technical Security. The ECtHR and CJEU hold that technical security protection extends beyond classic ‘negative’ human rights, mandating states to refrain from infringement, to ‘positive’ rights obligations to proactively ensure protection through legislation. Council of Europe and EU Member States as well as the EU legislature must ensure protection through legislation and meaningfully enforce citizens’ enjoyment of positive fundamental rights. Over the decades, the ECtHR has developed a ‘fair balance’ test with roughly five criteria that help to evaluate the existence of positive obligations for legislatures: i) the essence of a fundamental right is impaired; ii) the complexity of the topic at hand; iii) the existence of a European consensus on positive obligations; iv) whether a collision with other fundamental rights is at stake, and v) the vulnerability of citizens.

On the few occasions the ECtHR and CJEU have had an opportunity to rule more specifically on cases with a technical security dimension, the two courts established concrete principles and measures that EU and national legislatures need to take into account to meet fundamental rights requirements. ECtHR I. v. Finland of 2008 was the first case in which the ECtHR formulated a positive obligation to legislate and enforce technical security. Effectively, the ruling provided constitutional recognition to the European data protection regime, in particular article 17 DPD on data security. The Court said that compensation schemes after data breaches are not sufficient in light of the ECHR; ex ante protection is a fundamental rights requirement. In CJEU Digital Rights Ireland of April 2014, the CJEU annulled the entire Data Retention Directive. As it was the first ruling to ever annul an entire EU Directive solely on failures to meet fundamental rights safeguards, it most probably will play a central role in the development of EU fundamental rights law in years to come. The lack of robust legal safeguards on the security of communications security was one of the four main reasons for invalidating the entire Directive. The A-G opinion in CJEU Digital Rights Ireland suggested leaving the Directive intact and
mandating the enhancement of certain provisions, as most Member States had provided for access and security legislation in national law. But the CJEU left no doubt that the EU legislature bears full responsibility for protecting communications security in EU law.

In CJEU Digital Rights Ireland, the Court develops a new conceptual framework with regard to positive obligations to legislate network and data security (art. 7(a) DRD) by the EU legislature. The CJEU rejected the lack of “clear and precise rules” and “sufficient safeguards” in the combined regime of the Data Protection Directive, the E-Privacy Directive and article 7 of the Data Retention Directive. As such, the CJEU directly questions current legal provisions adopted in these policy cycles, and indirectly in the other policy cycles identified in Part I of the study. The CJEU gave two broad reasons for invalidating the data security provisions in the Data Retention Directive: i) a failure to establish law “specifically adapted to ensure full integrity and confidentiality”, and ii) failure of the law to ensure “compliance by an independent authority” as required by article 8(3) of the EU Charter.

**Laws Specifically Adapted to Ensure Full Confidentiality and Integrity.** The ECtHR and the CJEU explicitly demand a strict stance from the EU lawmaker going forward: legislation must be in place to safeguard against “any unlawful disclosure” (ECtHR) and ensure “full confidentiality and integrity” (ECtHR). The CJEU develops a new set of criteria to evaluate positive obligations for the EU legislature and connects the framework to the first two security attributes of the c.i.a.-triad. From now on, three criteria determine whether technical security must be ensured in EU legislation: a) information quantity; b) information sensitivity, and c) the risk of abuse of the information. Applying these criteria to the joint approach of the Data Protection, E-Privacy and Data Retention Directives, the CJEU finds that the Data Retention Directive does not ensure a “particularly high level of protection and security”. The Court said
that reliance on economic considerations of market operators and self-regulation does not suffice in this case. While not referenced, the CJEU Frontex case had already established that self-regulation and delegation are no options for the EU lawmaker when fundamental rights are at stake, particularly privacy and data protection. Although case documentation is unclear about this, the fact that the EU Commission appointed a Data Retention Expert Working Group, mostly consisting of law enforcement officials and regulated telecommunications operators, which came up with a set of compliance recommendations for the companies that retained communications data did not satisfy the CJEU.

The study argued that these new fundamental rights requirements challenge standard practices in EU legislation uncovered in Part I: the security provisions in the Directives held void in CJEU Digital Rights Ireland contained similar wording as can be found throughout the five policy cycles. Details are usually either delegated to the European Commission without further guidance how to balance the c.i.a.-triad attributes, or are delegated to self-regulatory bodies. These standard approaches, along with merely cross-referencing to the Data Protection Directive, fail to meet fundamental rights safeguards in specific instances. The study suggested that the insights from security economics scholarship fit well into the view of the court that economic considerations alone did not provide sufficient safeguards. With CJEU Digital Rights Ireland, the EU lawmaker must ensure full communications confidentiality and integrity on fundamental rights grounds: market failure becomes a fundamental rights issue when the factors of information quantity, sensitivity and abuse risks apply to a legal instrument adopted by the EU lawmaker.

The positive obligations established in ECtHR I. v. Finland and CJEU Digital Rights Ireland have elevated private communications security to a positive fundamental rights obligation. But with only a handful of specific rulings, the
doctrine is still in its infancy. The study proposed to examine the extent to which the new positive obligations formulated by the courts can be extrapolated to a substantive conceptualization of communications security for the EU lawmaker. To this end, the chapter analyzed two interconnected subthemes: i) the living instrument doctrine vis-à-vis the emphasis in CJEU case law and EU legislation towards data protection and ‘actor’-based scope; ii) communications secrecy as an ‘objectified’ first line of defense.

*Living Instrument Doctrine: A Functional Approach to Scope.* The European fundamental rights framework affords protection that is “practical and effective” and “dynamic and evolutive”, in the words of the ECtHR. The study analyzed the somewhat different approaches to dealing with rapid socio-technical change by the ECtHR and CJEU to further situate the instrumental role of communications security in fundamental rights law, and the scope it should be afforded.

As noted, the ECtHR employs the “living instrument” doctrine to align ECHR protection to emerging communications technologies. The 2013 *ECtHR Michaud v. France* and 2015 *M.N. a.o. v. San Marino* rulings explicitly adopts a content- and actor-agnostic approach to the protection of private communications under art. 8 ECHR. Private communications are protected, regardless of the sensitivity of information or the means of communication. Even though ECtHR case law is an integral part of the EU acquis, the CJEU appears to place considerable weight on the new article 8 EU Charter that has recently established the fundamental right to data protection. The dynamic “living instrument” doctrine has ripened over decades. The CJEU’s data protection approach, however, can be criticized for the same reasons as found in Part I of the study. The conception of ‘personal data’ is fiercely debated in the ongoing legislative saga on data protection reform. Moreover, the rights to communications secrecy, privacy and communications freedom afford a
broader protection than ‘personal data’ protection. In addition, the data protection right in art. 8 EU Charter is formulated relatively weakly in comparison to its broader privacy counterpart in art. 7 EU Charter. For all these reasons, the “living instrument” doctrine serves as a more robust anchor for conceptualizing communications security in terms of scope and underlying values.

The study argued that the EU lawmaker should address the problems arising around the legacy of ‘actor’-based scoping definitions observed in Part I of the study. Several core EU communications security provisions do not live up to their intended effect upon adoption, such as the data breach notification of the Telecoms Package, of which the EU Parliament intended a broad scope but only late in the process realized would only cover the narrow set of actors covered under the Telecoms Package. The case studies further substantiate this observation by pointing at the scoping arrangements in the eIDAS Regulation and the NIS Directive. The study proposed that fundamental rights concepts of “first line of defense” and “living instrument” can inform a functional approach to communications security legislation. A functional approach towards legislating communications security can overcome aforementioned concerns: rather than focusing on a predetermined set of market operators, legislation should identify the entire communications value chain, develop a normative understanding of the underlying values at stake and safeguard these underlying values.

The study also argued that the fundamental rights scope of communications secrecy and one of its central tools, technical security, should be broadened. The positive obligations in horizontal relations are increasing in relevance. Among the developments to support this statement are privatization of telecommunications, technology convergence, automated processing, cloud computing, pervasive passive and active network surveillance, the increase in
interdependences between private communications security providers and the falling costs of attacking communications through surveillance and cybercrime. With such developments, the traditional separation between information at rest and in transit may no longer provide the ‘practical and effective’ protection mandated by the ECtHR. The “first line of defense”, “living instrument” and “functional approach” concepts can inform such broader protections. The study proposed to investigate whether the technical concept of the end-to-end principle can inform legislating communications security in the ‘cloud’ communications case study of chapter 9.

*Communications Secrecy: A Constitutional First Line of Defense.* Confidentiality interests around state surveillance of citizens and organizations – first trade secrets and later communications freedom and privacy – have traditionally formed the core of the constitutional protection for communications. Both in vertical and horizontal relationships, the ECtHR holds that communications confidentiality should be ensured regardless of the intent or content submitted. The underlying rationale to warrant such protection is that communicants entrust communication to an intermediary, thus losing control in relation to the intermediary or third parties.

In several cases, the ECtHR has ruled that communications deserve protection regardless of their context or intent. In *ECtHR Kopp v. Switzerland* and *ECtHR Lüdi*, the Court afforded fundamental rights protection against infringements by observing the technological aspects of communications security before observing the intent or context of the content communicated. Several authors have observed that when the Court focuses on communications secrecy, it ‘objectifies’ the protection of correspondence. Only in a next phase of communications secrecy judgements are intent and context scrutinized through well-established theories around justifications for fundamental rights infringements, such as necessity, proportionality and subsidiarity. Thus,
communications secrecy functions as an ‘objectified’ first constitutional line of defense against unlawful breaches of communications. In other words, communications secrecy is vital to fundamental rights protection, regardless of intent and context. With these cases, as well as ECtHR Craxi II and CJEU Digital Rights Ireland, the ‘objectified’ protection of communications extends after the communication has ended. Even if the surveillance of one particular suspect (for instance, by law enforcement authorities) was justified, communications secrecy also protects against unlawful disclosure to third parties (such as the press). Conversely, as held in ECtHR M.K. v. France, technical security should not replace privacy and communications freedom scrutiny. France’s view that fundamental rights had been protected through technical security, which then allowed for storing and processing on vast amounts of sensitive data, fails under art. 8 ECtHR. The often heard argument that it suffices to protect the technical security interests of users and thus re-orient fundamental rights protection to regulating access conditions rather than collection itself has never satisfied the ECtHR.

Finally, conceptualizing communications security as an objectified first line of defense protects users against arbitrary national security interferences. As became particularly evident in the case study on operation MUSCULAR, a lack of communications security protections may create surveillance incentives on points in the networked communications environment least expected. The important consequence of a failure to protect against arbitrary interferences is the mere fact that it increases the threat of being exposed to secret surveillance that is not “in accordance with the law”. In other words, to create regimes for legitimate surveillance under the rule of law and in line with fundamental rights, communications security protection must be in place to serve as a first line of defense, especially against passive mass surveillance.
In sum, the study concluded that communications security will enjoy an increasingly broad level of protection under fundamental rights law and that the EU lawmaker must take up its ‘system responsibility’ to keep the EU acquis in line with long existing and relatively young fundamental rights requirements.

**Systems Design Perspectives**

Part I of the study observed that the c.i.a.-triad formed the basic conceptual framework for legislating communications security in the early 1990s. But the underlying concepts and theory have largely been forgotten, as the EU lawmaker copies former concepts into new legislation without proper consideration or providing normative guidance on how to balance confidentiality, integrity and availability in various use contexts of networked communications.

In chapter 5, the study established that the c.i.a.-triad forms a generally accepted and employed conceptual framework in computer science. To assess the viability of the c.i.a.-triad as a conceptual framework for legislating communications security, the study examined the concept as well as a series of concepts for designing systems security, such as security requirements engineering and multilateral security requirements engineering. The study finally discussed structural reasons why security fails, identifying four broad classes: surveillance, user, technology and market failure.

**The Technical Conception of ‘Security’: The c.i.a.-triad.** The c.i.a.-triad’s origins can be traced back to the mid-1970s. Over the years, different concepts have been suggested in order to extend the security attributes confidentiality, integrity and availability – such as reliability, authenticity and non-repudiation. The technical literature seems to arrive at a consensus that complete theoretical frameworks are extremely complex, and that the c.i.a.-triad therefore may serve
as a basic conceptual framework in the real world of systems design. Further complicating the framework would add unnecessary complexity to the relative clarity of the c.i.a.-triad. In Part II of the study, Pfleeger’s definition of computer ‘security’ was used as a conceptual starting point:

- **Confidentiality** – assurance that data, programs, and other system resources are protected against disclosure to unauthorized persons, programs, or systems;
- **Integrity** – assurance that programs, or systems protect data, programs, and other system resources are protected against malicious or inadvertent modification or destruction by unauthorized persons, programs, or systems;
- **Availability** – assurance that use of data, programs, and other system resources will not be denied to authorized persons, programs, or systems.

The study argued that the c.i.a.-triad suffices as the central anchor of a conceptual framework for EU legislation. For legislative and policy purposes, the added concepts in the computer science literature may be subsumed under the c.i.a.-triad’s attributes. The attributes of the c.i.a.-triad, however, do require further specification depending on the regulatory instrument and communications use under consideration. Technical and normative evaluation of the confidentiality and integrity interests at stake will differ substantially per EU policy cycle identified in Part I of the study. The fundamental rights evaluation of the c.i.a.-triad is a case in point. The study also observed that technologists and policymakers may have different connotations with the elements of the c.i.a.-triad, pointing at different conceptions of whether communications confidentiality also includes the metadata of communications. In fundamental rights, this certainly is the case, but it is very unclear whether technologists are aware of such requirements outside the realm of systems design. Such conceptual differences, a lack of understanding of the

---

774 Pfleeger 2003, p.504.
fundamental rights dimension of the c.i.a.-triads’ attributes, perhaps a lack of incentive for value-sensitive design and resulting misunderstandings between different communities can have real consequences. In global governance fora such as the Internet Engineering Task Force, the Internet Architecture Bureau and other standardization bodies, the number of fundamental rights experts is minimal. EU lawmaking lacks technical experts to consistently inform policy debates. The EU lawmaker needs to be aware of these nuances and lack of specific expertise in each respective policy arena. Instead, EU law usually refers such details without further specification to democratically unaccountable organizations. Recital 16 of the eIDAS Regulation is but one example, in which the EU lawmaker defers the formulation of voluntary security requirements for electronic identification in the private sector to a public-private consortium (STORK) funded by the European Commission.

Systems design theory instructs that merely stating the security attributes confidentiality, integrity and availability – as is done in several EU policy cycles – does not suffice. In Pfleeger’s definition of the c.i.a.-triad, the word ‘authorization’ mentioned under all three security attributes points at the necessary negotiation implicit in the c.i.a.-triad: the determination of the conditions and entities that may disclose, modify, or access. Such authorization is critical in systems design, especially when the underlying interests in a security system conflict. These authorizations are formulated after negotiating the ‘security goals’, or ‘security requirements’ of a system. In systems design theory, law has long been recognized as a primary source – along with design choices, contract and consent – of these negotiations. But the historical analysis of Part I pointed out that EU legislation often fails to provide such specific authorizations, let alone substantive or procedural guidance.

Security requirements engineering is one of the ways of eliciting more specific security goals. Its engineering methodologies instruct that requirements must
be stated, as well as prioritized and enforced, to give a systems security policy any meaning. In systems design, detailed procedural models have been developed to identify the underlying values and conflicting interests of stakeholders, resolve conflicts and prioritize outcomes, identify threats and enforce the requirements upon deployment. The method ‘multilateral security requirements engineering’ assumes that the underlying interests of stakeholders in any security system conflict. This is not seen as a problem, but as a necessary assumption for engineering security solidly. Conflicting interests must be formulated, negotiated and after reaching consensus, all stakeholders must be able to enforce the agreed protection goals.

Engineering systems and legislating communications security are inherently different processes. Expecting both systems designers and lawmakers to perfectly adopt each other’s theoretical methods is unfeasible. Nevertheless, the study concluded that the suggested field of security requirements engineering holds several valuable lessons for legislating communications security. Interests conflict, in any system, and conflicting interests need to be made explicit. In engineering, law and other policies are seen as primary sources to negotiate such conflicts. But EU law hardly specifies nor negotiates such differences. The study concluded that the EU lawmaker would benefit from a more systematic approach to policymaking that draws inspiration from security requirements engineering. The cases studies of Part III further develop these insights.

Security Failure: Surveillance, Users, Technology, Markets. The study examined the deeper causes of communications security incidents. The history of communications protocol design is littered with examples on the deliberate subversion, delay or rejection of widespread communications security technologies to enable government surveillance. The deliberate weakening of the GSM standard is a case in point, discussed in Part I. The crypto wars of the
1990s, also discussed in Part I, have led many engineers to believe that these issues had been resolved by perfect encryption technologies, available to privileged users that had the skills, technologies and time to secure their communications. Set aside the serious usability drawbacks of encryption, the disclosure by Edward Snowden of operations such as BULLRUN and EDGEHILL have driven the point home that many encryption solutions that we rely on have been manipulated and can be subverted, and should consequently be considered insecure.

Communications security can fail because of user behavior and technology, too. Managing and enforcing security is complex and time-consuming, even for the most experienced and technologically savvy engineers and users. The complexity of ICT systems can become quite extreme, for example in the case of the millions of lines of code and thus potential bugs in contemporary operating systems. In such situations, the average user cannot be held responsible for protecting his or her own communications security, which further emphasizes the fundamental rights duty to protect users.

Thus, often technology itself is an important cause for failure. Apart from complexity, legacy still plays a vital role in this respect. Core communications protocols of the networked environment, such as the Transmission Control Protocol (TCP) and Internet Protocol (IP), were designed with availability and connectivity as the leading principle. Confidentiality and integrity interests have not been a core concern in these leading communications protocols. Interconnectivity and soft- and hardware complexity needs to be tolerated to a certain extent going forward, if we are to reap the societal benefits of technological experimentation. Nevertheless, in technical communities a new consensus is emerging that communications security should be protected more robustly in technologies themselves. Over the last decades, dozens of proposals have been made to update the security of these core protocols in order to build
end-to-end security into the networked environment. End-to-end security is a design principle that seeks to ensure that only the sender and the recipient of a particular communicative act can decide upon conferring authorization under the c.i.a.-triad. Recently, particularly in response to Snowden’s disclosures, Internet governance bodies such as IETF, IAB and W3C have released statements that communications should protect integrity and particularly confidentiality by default. The EU lawmaker faces a quite straightforward choice in this respect: following a future trajectory that aims to secure networked communications against a wide range of adversaries, or maintaining a status quo in which many adversaries – including cybercriminals, intelligence agencies, corporate dataminers and then some – can exploit these legacy vulnerabilities, deliberate backdoors and unintended weaknesses in communications security. These dynamics are further explored in the case study on ‘cloud’ communications of chapter 9.

Finally, market failures are a crucial root cause for security breaches. Many serious security incidents do not have complex technical root causes. Fixes and solutions already exist to many systematic vulnerabilities across the communications security ecosystem, off the shelf, as well as updates to insecure Internet protocols still in wide use today. Security economics scholarship explains how systems security is often a problem of perverse economic incentives. It is rational economic behavior to underinvest in security: organizations that supply ICTs rarely bear the cost of failure; ICT customers do. Using economic theories such as information asymmetries, lock-in, negative externalities and liability dumping, security economics has explained various persistent security failures throughout the networked computing and communications environment. These market failures should be addressed through legislative intervention aimed at aligning persistent perverse incentives on the supply-side of communications security markets and information asymmetries harming the demand-side. The HTTPS
communications case study of chapter 8 delves deeper into the market incentives underlying communications security failures and how the EU lawmaker could respond to them.

Security economics scholarship has found market failures in leading security industries such as online banking, operating systems development and electronic health care and enjoys some traction in EU policymaking. The three classes of regulatory intervention mentioned in Part I have emerged from security economics theory: i) transparency obligations; ii) security requirements, and iii) liability arrangements. However, as observed in part I, the details of security economics provisions are often watered down considerably in the legislative negotiations between the EU institutions.

Political Perspectives

Chapter 6 of the study examined the relationship between communications security, surveillance and the political conception of ‘security’ to provide deeper understanding as to why systems fail. Examining these issues also provided deeper insights into whether communications security protection through EU legislation is politically feasible. Chapter 6 described the political conception of security through a political and social science literature review.

Along with the technical conception of ‘security’ researched in chapter 5, the longstanding political conception of ‘security’ moved into the area of legislating communications security in the early 1990s. The political concept of security appeals to basic human emotions and is intrinsically connected with the traditional function of the nation state. Security in its political manifestation carries divergent meanings and often unarticulated underlying agendas. Some of these were described in chapter 6.
**Subjective security.** Several modalities of political security were distinguished, including objective vis-à-vis subjective and material vis-à-vis procedural security. The study observed how subjective and procedural security increasingly seems to trump objective and material security in a wide range of policy areas. The study has linked the subjective and procedural turn in security policymaking to developments in contemporary global, technology-mediated and highly complex (post-)modern societies. These changes in human organization are increasingly beyond the control of any polity – be it a single legislative system, state, or community. With current institutional structures unable to address these broad societal shifts, anxieties around agency are translated into political security concerns to create an appearance of control. If appearance trumps actual agency, objective and material security is not what is at stake in legislating communications security. For citizens and elected officials alike, what may matter more is the appearance that insecurities are under control – a ceremonial act of security policymaking.

*’Cyber’ Securitization.* The study outlined theories around the discursive analytical tool of securitization to further understand the subjective and procedural turn in security policymaking. Securitization theory describes three stages of political discourse – non-political, political and securitized – and observes that once a policy topic has reached the third stage of securitization, facts become almost irrelevant. For this to occur, issues must be framed as i) imminent and existential threats, ii) to a significant collective and iii) by a potent actor that is accepted by surrounding communities. The political incentives for securitization are immense, as succeeded securitization effectively captures a policy space, and enables realization of political and economic agendas while lowering the standards on legitimacy and accountability. The literature identifies influential governmental and corporate representatives as primary securitizing actors, followed by mainstream media
and experts. Successfully securitized policy ‘sectors’ include defense, counter-terrorism, law enforcement, the economy and religion.

In recent years, many authors claim ‘cybersecurity’ must be added as a successfully securitized sector. While the Snowden revelations would certainly support such claims at first glance, most analyses in the literature exclusively cover the US legal and political system. Here, national security is the sole competence of the Federal government, in particular the Executive branch. The way communications security and national security relate to one another at the level of the EU legislature plays out in less evident ways. The historical analysis of Part I illuminated that a national security capture can be observed at several critical moments during the EU legislature of the last three decades. The EU lawmaker still lacks competence to legislate in matters framed as national security issues, but the EU Charter of Fundamental Rights may have changed the role EU institutions, notably the CJEU, will play in the future.

The observations of chapter 6 increase understanding of the historical analysis of Part I, and of future feasibility of EU legislative approaches. Firstly, a political science perspective on EU security policymaking explains the prevalence of cybercrime policy at the EU level. While deterrence as a security doctrine is known to have limited effect, EU criminal lawmaking creates an appearance of control as institutions are seen as acting on cybercrime. The study pointed at several developments in EU and national policymaking that support the impression that cybercrime has been successfully securitized at the EU level. Secondly, the multi-layered national security capture of EU communications security policymaking – explicitly, implicitly and covertly secretly – had been observed in Part I. The insignificant EU response to the Snowden revelations, which implicated European Member States too, can be seen as a result of implicit capture of the EU lawmaker by national security interests. As soon as one EU Commissioner spoke up about the revelations,
then EU Commission President Barroso immediately responded by evoking the EU Treaties and stating it was beyond the EU to deal with surveillance failures on communications security.

**The implicit politics of technology policymaking.** Across its institutional branches – the Parliament, Commission and Council – the EU lawmaker deeply depends on the input of technical experts. Also, the EU lawmaker is reluctant to fully engage with the technical aspects of technology policymaking. Technical experts often have significant interests with regard to regulatory topics, be it because of their employment or personal politics. The resulting implicit politics of technology policymaking may lead to long-term implications for EU communications security lawmaking, and does contextualize some of the recent legislative developments observed in Part I, especially with regard to the delegation of the details of legislative provisions to either standardization or even industry self-regulatory institutions, as happened with the eIDAS Regulation.

The prevalence of subjective over objective security, ‘cyber’ securitization and the implicit politics of technology policymaking all create perverse incentives on part of the EU lawmaker to protect private communications security through EU law. Often, meaningful protection of private communications is not at all what (cyber) security is actually about. Rather, under the guise of security, economic and strategic political agendas are secured. These deeper political dynamics come to the surface in the case studies of Part III.

### 10.3. Part III: Case Studies for the EU Lawmaker

*Model and Methodology*
Based on the earlier findings of Part I and Part II, the study developed a procedural model for analyzing and determining whether the EU lawmaker should protect private communications security through EU law. The model consists of the following steps:

1. Map the functional value chain of relevant communications uses;
2. Identify systemic vulnerabilities;
3. Analyze market and surveillance incentives;
4. Operationalize the c.i.a.-triad and fundamental rights perspectives;
5. Examine the available technical solution;
6. Assess the role of EU law so far and offer recommendations.

The study applied the model in two case studies on HTTPS and ‘cloud’ communications. HTTPS and the ‘cloud’ are present in everyday communications use cases. HTTPS is an absolutely critical communications security technology that enables a thriving E-Commerce market, but the protocol is systemically insecure and has been severely breached over the last years. While several solutions can fix the most damaging properties of HTTPS and its Certificate Authority infrastructure, updates do not happen and severe breaches continue. In the second case, the Snowden disclosures have made clear that the rapid transition of networked communications and computing in general from owned local devices to infrastructure at a distance – or the ‘cloud’ – has serious implication for information security, autonomy and fundamental rights. The case study focuses on the MUSCULAR surveillance program, run by the intelligence agencies NSA (US) and GCHQ (UK) and disclosed by Edward Snowden.

The HTTPS case study emphasized the market incentives for providing HTTPS and applied security economics methodologies alongside conventional legal methods. The ‘cloud’ case study employed methods from computer science – primarily threat modeling – along with fundamental rights analysis, focusing
on surveillance incentives. Both case studies have been workshopped and
published across academic disciplines and add another inter-disciplinary layer
to this study on EU communications security law. Both case studies ultimately
assess how EU law should protect private communications security – the
central research question of the entire study – in specific communications use
cases that everyone faces daily across the networked communications
environment: web browsing and cloud computing.

HTTPS – Communications Security in Web Browsing

HTTPS has become a de facto standard for securing web communications,
essential to protect general web browsing activity against disclosure to or
modification by an attacker with access to communications. However, major
security breaches have and continue to expose systemic vulnerabilities in this
critical cybersecurity technology.

The case study identified four central stakeholders that together form the
functional value chain of HTTPS communications: certificate authorities (CAs),
website operators, browser vendors and users. Functional value chain analysis
uncovered a number of systemic vulnerabilities in HTTPS communications.
The security of the entire ecosystem depends on the security of one of the
hundreds of CAs (‘weakest-link’). Browsers are not really able to revoke trust
in major CAs (‘too big to fail’). Most website operators still choose not to offer
HTTPS or implement it poorly. In addition to CAs, website operators and
browser vendors thus contribute to the status quo. All breached CAs initially
managed to conceal serious security incidents, which begs the question how
many CA breaches have gone unnoticed to the general public. Meanwhile, the
liability of security incidents is dumped on users, even if they cannot
reasonably be expected to make informed decisions based on the security
signals of browsers, lengthy terms and conditions or knowing how to remove

332
hundreds of irrelevant CAs from their browser settings. Operationalizing the c.i.a.-triad explains how the communications security interests conflict among stakeholders in the functional value chain. In many scenarios, they must choose between allowing a breach of confidentiality or availability.

Without HTTPS, confidentiality and integrity of web browsing cannot be assured. The CJEU Digital Rights Ireland criteria of sensitivity, quantity and risk of abuse applied to web browsing show that properly configured HTTPS communications protect user privacy, communications freedom and a number of associated fundamental rights. Even if communications metadata are not protected, HTTPS serves as one of the only lines of defense to protect fundamental rights against arbitrary interferences when browsing the web. HTTPS thus deserves strict protection by the EU lawmaker and mandatory deployment in numerous communications contexts.

Empirical analysis of the economic incentives of website operators, certificate authorities and browsers vendors proved vital to analyze the legislative response of the EU. The HTTPS market is highly concentrated. Nonetheless, the market is characterized by very large price differences among suppliers, with limited to no price competition. In other words, the systemic vulnerabilities may actually benefit rather than hurt dominant CAs that have become too big to fail. This is all the more relevant, as technical and self-regulatory solutions need to be implemented by the very same market leaders that lack an incentive to actually augment the HTTPS status quo.

In terms of solutions, the EU has opted for a legislative response, while the US seeks resolve in self-regulatory and technical approaches. How do the different technical and regulatory solutions deal with the market failures of information asymmetry and negative externalities? In general, the technical proposals are much more promising to address the systemic vulnerabilities of HTTPS. But as
the dominant CAs lack economic incentives to augment the security of HTTPS as it stands, none of the proposals are anywhere close to large-scale implementation, let alone adoption. The standard repertoire of regulatory options to remedy these failures are present in the legislative approach of the EU: liability, security breach notifications, minimum security requirements. But the Commission proposal for the eIDAS Regulation already failed to consider the role of all stakeholders in the HTTPS value chain as it merely focuses on CAs. The April 2014 EU Parliament amendments and finally adoption of the eIDAS Regulation made matters much worse. All provisions were considerably watered down. The industry self-regulatory body is even named in the recitals as a leading voice to assist in determining the details of the security requirements and breach notification provisions. Overall, the Regulation does not address systemic vulnerabilities and persistent market failures. The legislative debate shows elements of an implicit politics in technology policymaking as well as successful lobbying from the same industry that the Regulation in its initial proposal sought to regulate. Economic interests have dominated the legislative debate, while positive fundamental rights obligations to secure communications have not been part of the legislative debate at all.

The Snowden Files – Communications Security in the ‘Cloud’

The migration of computing from local devices to the ‘cloud’ has major implications for end user communications security and the enjoyment of fundamental rights online. Snowden’s disclosures, along with a number of security incidents at cloud providers only briefly discussed in this chapter, have driven the point home that customers lose control and oversight as soon as they entrust their communications and data to the ‘cloud’. Unprotected communications run into significant risk of being captured under operations such as MUSCULAR, the program extensively discussed in this case study, as
well as countless others also outlined in this chapter. Such major breaches have been occurring on an unimaginable scale.

The functional value chain of ‘cloud’ communications extends beyond the client-server communications path of the HTTPS case study into the network of datacenters behind the front-end servers of ‘cloud’ providers – so-called intradomain cloud communications. Many ‘cloud’ services also offer communications services by opening up so-called interdomain communications paths between themselves and other service providers such as CDNs. Even a cloud provider can hardly tell whether a fiber intermediary or an Internet exchange is benevolent, malicious or coerced by a foreign government to cooperate in mass ‘cloud’ surveillance. Until the Snowden disclosures hardly any ‘cloud’ provider secured these communications properly. But end users depend on them for the enjoyment of their fundamental rights online – especially in the SaaS-models implicated in MUSCULAR. Even today, breaches of integrity and confidentiality remain unrecognizable from outside the ‘cloud’ (i.e. the user-, or general public facing server-side); only some ‘cloud’ providers have seriously stepped up efforts to secure the ‘cloud’ in intra- and interdomain communications paths. Whereas communications availability is a core interest and competitive concern for industry, and spectacularly maintained, communications integrity and confidentiality are major concerns unaddressed in the market for ‘cloud’ computing.

The case study applied the general ‘fair balance’ test of positive obligations in fundamental rights law to ‘cloud’ communications and found the test supports positive fundamental rights obligations to secure cloud communications through EU law. Applying the CJEU Digital Rights Ireland framework to MUSCULAR shows that Google and Yahoo! ‘cloud’ communications are extremely sensitive, occur in large quantities and the risks of abuse are manifold. Apart from communications metadata, MUSCULAR intercepted
communications contents, contact lists, chats, pictures, video and many other classes of communications data on a massive scale. Ensuring the full confidentiality and integrity of ‘cloud’ data will require the EU lawmaker to adopt legislation to meet its positive obligations. Also, EU legislation must play a role in securing the ‘cloud’, given the perverse market and surveillance incentives observed in the case study. Moreover, technology cannot save the day by itself. The access to ‘cloud’ communications must be brought within a legal framework and states should commit to fundamental rights safeguards. But the incentives for covert surveillance remain enormous, as long as ‘cloud’ communications are hardly protected in intradomain (for example, between datacenters of a single ‘cloud’ network) and interdomain (between providers or CDNs) communications paths.

10.4. Conclusion, Recommendations and Outlook

This study analyzed the following central research question: how should the EU lawmaker protect private communications security? This section formulates answers, recommendations, directions for future research and the outlook of EU private communications security law.

The study concludes that the EU lawmaker can and must augment private communications security and has launched legislative programs in all five EU policy cycles to do so. But the EU lawmaker does not integrate into its law- and policymaking several essential crucial fundamental rights, socio-technical and market developments, outlined in this study. Meanwhile, the importance of and our dependence on secure networked communications is only increasing over time. The study therefore recommends a fundamental reconceptualization of EU communications security law and offers five suggestions on how to reorganize its very foundations. At the same time, the study observes several
deeply perverse market, surveillance and political incentives that negatively impact the protection of private communications through EU law. As such, the short term outlook on the viability of the EU lawmaker to protect private communications security is sobering. On the longer term, fundamental rights as well as technical developments such as the Internet of things and the associated life-threatening risks of security breaches make more robust protection of private communications security inevitable.

For now, the EU lawmaker has yet to realize that protecting communications security is becoming a fundamental rights obligation. Case-law of European constitutional courts has started to establish positive obligations of the EU lawmaker to protect the enjoyment of fundamental rights through technical security legislation. And the “living instrument” doctrine will continuously extend fundamental rights safeguards to new ICTs and communications functions. Moreover, national security interests have exercised strong implicit and secret influence over EU communications security policymaking in the last three decades. In a time when the end users massively migrate their computing to the ‘cloud’ and the costs of communications surveillance and conducting cybercrime have dramatically fallen, EU law has offered little counterbalance in terms of legal and technical safeguards. Instead, the EU lawmaker prioritizes availability interests and is hardly even trying to protect private communications security against arbitrary interferences on fundamental rights.

In terms of technologies, the EU lawmaker has systematically omitted to apply the same communications security standards to new technologies in the networked environment. An Internet access provider and ‘cloud’ provider offer many similar services (such as e-mail), but where the Internet access provider must meet (for example) the communications confidentiality requirements of the E-Privacy Directive, a cloud provider falls outside the scope of that instrument and thus faces hardly any legal obligations to offer communications
security for end users. Moreover, persistent market failures in the provision of communications security have not been taken into account, as demonstrated in the HTTPS case study. A certificate authority can still dump most of the damages resulting from a communications security breach on customers, regardless of several major breaches of HTTPS communications. Website operators are still not mandated to deploy HTTPS, nor have web browser vendors been obliged to follow Mozilla’s leadership of implementing certificate chain of trust transparency. Promising technical updates to the flawed authentication mechanisms in HTTPS are available, but not implemented because dominant CAs actually benefit from the flawed status quo.

These are just some examples of the fundamental flaws in current legislative approaches of the EU. As long as the deeper conceptual shortcomings and developments described in this study are not addressed, EU communications security law will prove inadequate to comprehensively protect private communications security. Thus, EU communications security law needs a fundamental conceptual revision. Part II and III combined theoretical and practical insights to examine what can be done to address the status quo.

**Recommendations.** In conclusion, the study offers five general recommendations the EU lawmaker should take into account. These five recommendations lead to a general conclusion on how the EU lawmaker concretely should implement meaningful protection for private communications security through EU law.

First, the EU lawmaker should conceptualize communications security as a constitutional first line of defense. EU law must afford basic and comprehensive communications security protection to protect end users against arbitrary fundamental rights interferences, regardless of the type of
communication or provider involved. More concretely, in legislative debates that touch upon communications security, the EU lawmaker should specifically identify the underlying values of communications confidentiality, integrity and availability and offer normative guidance in balancing these security attributes when they conflict. The EU lawmaker is increasingly constitutionally bound to meet its positive obligations, or ‘system responsibility’, from a fundamental rights perspective.

The status quo in policymaking and lack of a fundamental rights vision on part of the EU lawmaker will prove unsustainable and legally unacceptable in future legislation. Since the 2014 ruling CJEU Digital Rights Ireland, the EU lawmaker must adopt “rules specifically adapted to ensure full confidentiality and integrity.” In particular, the EU lawmaker is responsible for actively engaging with communications security when the CJEU Digital Rights Ireland criteria of information quantity, sensitivity and risk of abuse are at stake. The EU lawmaker must face its fundamental rights obligations going forward and structurally ensure communications confidentiality and integrity, rather than merely prioritizing availability and referring to business continuity in the digital economy. Even if fundamental rights do not provide sufficient political incentives to do so, ensuring business continuity in a digital economy will increasingly require a more prominent role for confidentiality and integrity assurances. The c.i.a.-triad, as employed in the case studies of Part III, offers a suitable conceptual framework to uncover the underlying values of communications security and meet fundamental rights obligations. When the CJEU Digital Rights Ireland criteria of information quantity, sensitivity and abuse risks are at stake, the conventional hands-off approach of the EU lawmaker to mandate ‘organizational and technical measures’ and allow the details to be determined either by the European Commission, self-regulation, standardization or the invisible hand of the market fails to meet fundamental rights requirements.
Second, the exclusion of national security from the competence of EU lawmaking in the EU Treaties needs nuance going forward. Too often, national security functions as a strawman argument for the EU lawmaker to shy away from the vexing confrontation of national security and private communications security. In addition, a crucial weakness in EU law is that national security is not properly defined. Across the five EU policy cycles, national security exemptions exist, but if the scope of an exemption is unknown, it could overshadow the law itself whenever an intelligence agency frames a certain issue as a matter of national security. Since the adoption of the EU Charter in 2009, the EU lawmaker is required by fundamental rights law to protect private communications. With CJEU Digital Rights Ireland, the court has already shown its preparedness in filling the fundamental rights void in the EU. Limitless framing of private communications security protection as a matter of national security policy cannot and should not entail a complete disregard of the EU lawmaker. On the political level, the EU lawmaker has ample opportunities to effectively afford protection by framing private communications security as a policy space that affects innovation, consumer protection, trade secrets and fundamental rights as well. Shifting in doctrinal approach from deterrence to protection, hardening the security of networked communications paths along the functional value chain and keeping a close eye on the actual implementation of security technologies and protocols are some of key avenues the EU lawmaker can pursue. As the crypto wars of the 1990s are being revived by intelligence and law enforcement officials, the case study of operation MUSCULAR points at a wealth of arguments against deliberately weakening communications security on national security or law enforcement grounds, as well as the many still existing possibilities to conduct legitimate surveillance even if communications are encrypted end-to-end.
Third, the EU lawmaker should adopt a new approach on scoping EU communications security law. The EU lawmaker needs to include all relevant providers in the value chain of a certain communications use and focus on its function and the underlying values at stake. The current scoping arrangements – ‘personal data’ and ‘actors’ according to already existing EU laws – have led to fragmentation of EU law, resulting in a patchwork of end-user protection. The current fragmentation also limits comprehensive incentive analysis across sectors; for instance how the incentives structures of online banks, web browsers and a Certificate Authority interact as illustrated in the HTTPS case study. Moreover, only addressing parts of the functional value chain in legislation risks that vulnerabilities and breaches move onto the next link in the functional value chain. Operation MUSCULAR deliberately attacked intradomain and interdomain ‘cloud’ communications links, as these were the links in the value chain that enjoyed hardly any technical or legal protection, thus passively and arbitrarily intercepting communications metadata and content on a mass scale. End users should be able to rely on EU communications security law whether they use landlines, Skype or WhatsApp to make a call, or their Internet access provider or Yahoo! to send e-mail. In addition, the HTTPS and ‘cloud’ cases show that a broad notion of “end-to-end” encryption is needed. “End-to-end” encryption needs to cover the communications paths from a user through the front-end server of a ‘cloud’ provider, all the way through the back-end servers and the Internet backbone. Distinctions between data ‘at rest’ and ‘in transit’ no longer apply in networked communications, as duplication to back-up data and constant transit to leverage scarce network resources are inherent features of ‘cloud’ computing. Protecting private communications security requires a coherent, holistic approach with regard to scoping legislative action in EU law.

Fourth, the EU lawmaker should correct persistent market failures that lead to perverse incentives in security production. The EU lawmaker is the suitable
lawmaker to do so. In addition to aforementioned fundamental rights requirements, harmonizing the internal market, and intervening when markets fail, is a key objective of the EU. As communications security markets tend to be dominated by a few dominant providers that operate on an international scale, the EU lawmaker is in a much better position to augment communications security in terms of subsidiarity vis-à-vis its Member States. The EU lawmaker should develop methods to identify relevant markets and stakeholders, analyze the incentives for security, formulate the key objectives and results of legislative intervention and then craft appropriate legislative responses (if any); similar to the case study on HTTPS communications of Part III. As observed in Part I, security economics insights have started to become adopted in some of the EU policy cycles. But recent legislative developments show that the initially proposed security requirements, transparency obligations and liability arrangements have been watered down considerably, especially in the digital signatures and certificates and network and information security policy cycles. To address market failures, the EU lawmaker needs the entire class of security economics provisions in its toolkit, rather than a transparency obligation in one policy cycle, and a security requirement in another. In addition, as detailed value chain and market analysis should be done on a case by case basis, the enforcement and oversight structures that need to be in place are currently lacking across the five EU policy cycles – especially in the proposed Network and Information Security Directive.

Fifth, the analytical model for examining whether the EU lawmaker should protect private communications security in specific cases developed in Part III of this study offers refreshing insights. The model addresses the conceptual shortcomings found in Part I and II of the study by integrating obligations and insights from fundamental rights, the c.i.a.-triad, functional value chain analysis, security requirements engineering and security economics. In particular, the step-by-step model can help the EU lawmaker to develop a
systematic approach to policymaking. At the same time, different communications functions have their substantive specifics: the functional value chains, underlying values and competing interests, systemic vulnerabilities, as well as market and surveillance incentives are substantially specific to HTTPS vis-à-vis intra- and interdomain cloud communications. The case studies show that analyzing the role of the EU lawmaker in regulating HTTPS communications vis-à-vis ‘cloud’ communications is procedurally a similar analysis, but may lead to a substantially different set of solutions. In the end, the EU lawmaker also needs to evaluate the viability of legislative action on a case by case basis. To this end, the broad application of the analytical model of Part III beyond HTTPS communications and operation MUSCULAR in the ‘cloud’ seems promising, and is an obvious candidate for future research.

Synthesizing these five recommendations, the sketches of a new regulatory framework for EU communications security become visible. The EU lawmaker must depart from the current approach of fragmented policymaking across five policy cycles. Instead, the EU lawmaker must develop a coherent vision on how EU law copes with the structural and more incidental characteristics of legislating communications security, and focus on the former. For this to occur, the EU lawmaker needs to answer and agree upon core questions of law- and policymaking: what are the normative values and goals underlying EU private communications security law? After CJEU Digital Rights Ireland, confidentiality and integrity must form the cornerstone of such a normative value framework. Furthermore, the EU lawmaker needs to adopt a functional approach to protecting communications security end-to-end in line with the “living instrument” doctrine, while the analytical framework offered in CJEU Digital Rights Ireland can serve as a guiding normative baseline. If communications such as ‘HTTPS communications’ or ‘cloud communications’ are deemed sensitive, widely used (‘quantity’) and the risk of abuse is found apparent, assuring protection cannot be left to the market or self-regulation
alone, but require strict protection and sustained attention from the EU lawmaker.

The EU lawmaker can also provide for the concepts and tools to achieve these goals: map the functional value chain of specific communications functions, analyze systemic vulnerabilities, the market and surveillance incentives in these contexts and then reflect on the possible legislative interventions. The three classes of regulatory intervention that have been discussed in the study can be offered too: security requirements, transparency obligations and liability arrangements. The case studies argue that possible measures include end-to-end encryption, robust authentication mechanisms, security breach notifications, mandatory vulnerability reporting and liability arrangements that prevent damages being dumped on end users in terms and conditions. How these are applied must be decided upon on a case by case basis, depending on the prior analysis of a certain communications use case. As the study mostly adopted a conceptual approach, the precise formulations of these three classes of legal interventions (security requirements, transparency obligations and liability arrangements) need urgent research, especially from the perspectives of European and national private law. Also, structural enforcement will be key to achieving the broader goals tailored to more specific communications use cases, and must be provided for by the EU lawmaker. This requires more research into the allocation of responsibilities between different types of regulators – the legislature, enforcement agencies, courts, and the opaque role of the many different standardization bodies in the field, including the IETF, IAB, W3C, ETSI and IEEE. In sum, the integration of fundamental rights, 775 One recent and refreshing study from the perspective of private law comes from T.F.E. Tjong Tjin Tai et al. 2015. The reportresearches possible legal duties of care of private actors in four legal systems (The Netherlands, USA., Brazil, and the Czech Republic). The report studies these legal systems through the lens of three specific topics: the security of hardware and software, ransomware, and DDoS attacks. The study comes to similar conclusions as reached in this study in general, and in particular in the HTTPS case study of chapter 9. See: <https://pure.uvt.nl/portal/files/5733322/Tjong_Tjin_Tai_cs_Duties_of_Care_and_Cybercrime_2015.pdf>, accessed 2 September 2015. See also Van Eijk et al. 2009.
security requirements engineering and security economics perspectives is the key to meaningfully protecting private communications security at the EU level.

Concretely, for these recommendations to be integrated in EU law, the EU lawmaker will need to adopt a proto-policy cycle that departs from the five policy cycles identified in Part I. Current legal instruments cannot address the inherent conceptual flaws of EU law. The data protection cycle seems inherently unsuitable to address the systemic vulnerabilities of cloud communications in the intra- and interdomain, because national security is explicitly excluded from its scope and as to content, it only covers data protection interests. The communications confidentiality safeguards of the E-Privacy Directive do not extend to ‘cloud’ providers, thus the Telecoms Package becomes an inherently unsuitable policy cycle to augment private communications security along the functional value chain. The NIS Directive is destined to fail, given the current political gridlock between EU institutions, the uncertainty whether ‘cloud’ providers are intended to be included in its scope at all and the very weak security requirements arrangements, let alone enforcement structures. Normative goals are not formulated, the scope will be limited, the provisions have been watered down considerably during the legislative debates and the oversight structures discussed continue to have little clout to meaningfully enforce communications security on the supply-side. Several issues need further research, as outlined below. Moreover, Member States seem not at all willing to hand over the keys to communications security protection to the EU lawmaker. Such political dynamics and the outlook for private communications security protection by the EU lawmaker are also discussed below.

**Outlook.** To assess whether the EU lawmaker is capable of the recommended fundamental reconceptualization and regulatory overhaul, the study engaged with political dynamics of EU communications security lawmaking.
Regulatory concepts and tools adopted during the first wave of communications regulation in the mid ‘90s cannot cope with a fundamentally changed networked communications environment today that stretches concepts and tools beyond breaking. From that perspective, the current shortcomings of the EU lawmaker are quite understandable. At the same time, a fundamental revision of EU communications security law as proposed by this study requires a substantial and structural political effort. New concepts and tools would have to be adopted in several policy cycles simultaneously, requiring sustained focus and a shared vision on what is at stake in protecting private communications security.

A vast body of political science literature has established that the concept of security appeals to completely different underlying values across technical and political communities. In framing communications security as ‘cyber’-security, EU communications security shows many signs of successful ‘securitization’, meaning a close relationship with national security and industry aiming to frame the policy space of systems security to their mutual benefit. Successful securitization, as many argue has already occurred in the US, implies that objective facts matter less than subjective processes – politicians prioritize the appearance of control over results.

The historical analysis of Part I and case studies of Part III indeed illustrate that protecting a conception of security that aligns with end user interests in fundamental rights and systems security may not be at the top of the EU’s political priorities. Current political dynamics seem to point at quite different ambitions of the EU lawmaker than protecting the communications security interests of end users. Security requirements are watered down, and availability and continuity of the economy are prioritized, rather than the confidentiality and integrity interests that need to be safeguarded through legislation, as the study argued. The scope of EU law still does not cover essential stakeholders in
communications value chains, and oversight mechanisms are sought to be placed within the national security establishment of Member States. To both Snowden’s disclosures and an evidently failing HTTPS communications ecosystem, the response of the EU lawmaker has been either weak or counterproductive, as concluded in the case studies.

Therefore, the study warns that entrusting the EU lawmaker with communications security policy runs a serious practical risk of lowering technical communications security protection in individual countries to a lowest common EU denominator. For many European countries, this has happened before with the EU Data Retention Directive and seems to be happening again with the eIDAS Regulation and the proposed ‘Network and Information Security’ Directive. The political and economic incentives to enable surveillance and maintain low regulatory requirements for corporations to secure communications are strong, even if the same incentives render networked communications highly vulnerable to cyberattacks and in breach of fundamental rights. While European fundamental rights courts are eager to protect the fundamental rights of end users, courts are confined to the cases they hear and often have their say many years after a particular piece of EU law was adopted. Meanwhile, Member States have already implemented fundamentally flawed EU law. After CJEU Digital Rights Ireland, several Member States still stubbornly disregard the ruling and maintain damaging data retention laws. More than 18 months after the ruling, the European Commission has not launched a single infringement procedure with the CJEU against a Member State that maintains the same data retention laws as before the landmark ruling. Rather, the European Commission seems to be considering a new Data Retention Directive. Eight years before and even after the ruling, the EU institutions seem prepared to do everything within their power to maintain a publicly controversial, heavily criticized by scholars and now annulled EU Data Retention Directive. The status quo is deeply
problematic and disregards the reality that after *CJEU Digital Rights Ireland*, the Court singled out the EU lawmaker as the institution responsible for safeguarding minimum constitutional requirements for fundamental rights and private communications security.

The coming years will prove what EU communications security law- and policymaking really is about. Since the 1990s, the EU claims that the stakes of protecting private communications security are “a pervasive quality necessary in modern society”\(^ {776}\) but actual EU law repeats history and keeps failing to meaningfully deliver on such grandiose claims. Why? Robust private communications security protection forces the EU lawmaker to confront broad and fiercely contested issues, such as market intervention, fundamental rights and the centrality of communications surveillance to what it means to be a nation state. Nonetheless, the EU lawmaker must provide coherent normative guidance by re-thinking the concepts, tools, provisions and enforcement structures of private communications security law- and policymaking. This requires a transparent debate on the normative imperatives of EU communications security law. No easy nor politically attractive task for an economic union that has only recently turned into a full constitutional order with the adoption of EU Charter in 2009, while EU skepticism grows and a ‘Grexit’ seems imminent and the United Kingdom – with its structural efforts to undermine private communications security since the 1990s – is openly discussing leaving the EU and fundamental rights treaties altogether. Recent developments in fundamental rights case law described in chapter 4, in particular *CJEU Digital Rights Ireland*, may give rise to some optimism in the longer term. Private communications security is vital for the enjoyment of fundamental rights, not only privacy and communications freedom, but freedom of association, of thought and a wide range of related fundamental

rights as well. From a fundamental rights perspective, history cannot repeat itself. But in the political arena, opportunities for capturing EU communications security law remain strong.

Ultimately, the EU lawmaker seems reluctant to meaningfully protect private communications security for end users. For the foreseeable future, a fundamentally flawed EU regulatory framework for private communications security protection underlies the networked communications environment used by every EU citizen, every day. Soon, for instance in the upcoming court cases on Snowden’s disclosures, European fundamental rights courts will mandate robust communications security protection through EU law. Maybe when our home appliances, pacemakers and cars are fully integrated to the ‘Internet of things’ – and it is not our data, but our physical security that is on the line – the political institutions of the EU will also see the urgency to start the full, systematic revision recommended by this study. When that time arrives, this study may offer some guidance on how the EU lawmaker should secure private communications.

* * *
References


359


Storm 2014 – D. Storm, 17 exploits the NSA uses to hack PCs, routers and servers for surveillance, 3 Jan. 2014, Computer World.


Legal texts

International

Universal Declaration of Human Rights.
International Covenant on Civil and Political Rights.

Council of Europe


Organisation for Economic Co-operation and Development


European Union, Charter and Treaties

Treaty on European Union (consolidated version 2012), C 326/01, 26 october 2012.
Treaty on the Functioning of the European Union (consolidated version 2012), C 326/01, 26 october 2012.

European Union, regulations and directives


The Netherlands

The United States
### Table of cases

**European Court of Human Rights**

- ECHR, Tyrer v. United Kingdom, No. 5856/72, 25 April 1978, par. 31.
- ECHR, Rotaru v. Romania, No. 28341/95, 4 May 2000.
- ECHR, Colas Est, 16 April 2002.
- ECHR, Christine Goodwin v. United Kingdom, No. 28957/95, 11 July 2002.
- ECHR, Muscio v. Italy, No. 31358/03, 13 November 2007 (inadmissible).
- ECHR, Copland v. United Kingdom, No. 62617/00, 3 April 2007.
- ECHR, Liberty et al. v. United Kingdom, No. 58243/00, 1 July 2008.
- ECHR, Iordachii and Others v. Moldova, no. 25198/02, 10 Feb. 2009.
- ECHR, Uzun v. Germany, No. 35623/05, 2 September 2010.
- ECHR, Telegraaf Media Nederland Landelijke Media B.V. a.o. v. The Netherlands, no. 39315/06, 22 Nov. 2012.
- ECHR, Peruzzo & Martens v. Germany, 7841/08 & 57900/12, 4 June 2013 (inadmissible).
- ECHR, M.N. and others v. San Marino, Application no. 28005/12, 7 July 2015.
- ECHR, Zakharov v. Russia, no. 47143/06, (ongoing).

**Court of Justice of the European Union**
CJEU, C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk, 20 May 2003.
CJEU, C-275/06, Promusicae, 29 January 2008.
CJEU, C-400/10, J. McB. v L. E., 5 October 2010.
CJEU, C-92/09 and C-93/09, 9 November 2010, Volker und Markus Schecke and Eifert.
CJEU, C-70/10, Scarlet v Sabam, 24 November 2011.
CJEU, C-584/10 P, C-593/10 and C-595/10, Kadi, 2013.
CJEU, C-355/10, Frontex, 5 September 2012.
CJEU, C-342/12, Worten - Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT), 30 May 2013.
CJEU, C-293/12 and C-594/12, Digital Rights Ireland Ltd, 8 April 2014.
CJEU, C-131/12, Google Spain, 13 May 2014.
CJEU, C-362/14 (Schrems v. Data Protection Commissioner), 2015 (ongoing).

Germany

Bundesverfassungsgericht 27 February 2008, decisions, vol. 120, p. 274-350 (Online Durchsuchung) [Online Search].
Bundesverfassungsgericht 2 March 2010, BvR 256/08 vom 2.3.2010, Absatz-Nr. (1 345), (Vorratsdatenspeicherung) [Data Retention].

Netherlands


United Kingdom


United States

United States v. Fregoso, 60 F.3d 1314, 1321 (8th Cir. 1995).
United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007).
United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008).
Prior Publications in the Thesis And Relative Contribution Co-Authors


Part of article included in chapter 8. Majority of text in article written by first author. Security economics analysis and technical solutions in paragraphs in article drafted by Asghari and Van Eeten. Parts included in section 8.2, 8.3. and 8.5. of thesis. Permission obtained for re-use in thesis.


Part of article included in chapter 8. Text in article written by first author. Parts included in section 8.1. and 8.2. of thesis. Permission obtained for re-use in thesis.


Part of article included in chapter 8. Majority of text in article written by Arnbak. Security economics analysis, technical solutions and lateral analysis in paragraphs in article drafted by Asghari and Van Eeten. Parts included in section 8.2, 8.3, 8.5 and 8.6 of thesis. Permission obtained for re-use in thesis.


In de informatiesamenleving van vandaag de dag is ons economische, sociale en politieke leven sterk afhankelijk van de beveiliging van elektronische communicatie. Tegelijkertijd staat communicatiebeveiliging voortdurend onder druk. De zorgen die al jarenlang geuit worden in academische en technische kringen zijn inmiddels door een reeks aan ernstige incidenten ook naar beleidsmakers en het grote publiek overgewaaid. Datalekken, cyberaanvallen en netwerkstoringen – in de publieke en private sector – zijn nu veelbesproken maatschappelijke problemen, in het nieuws en politiek arena’s over de hele wereld.

Twee incidenten die dit proefschrift uitgebreid onderzoekt zijn allereerst de surveillance- en hacking-operaties van Westerse regeringen, zoals onthuld door Edward Snowden. Op de tweede plaats bestudeert het proefschrift het cruciale communicatieprotocol HTTPS, dat beveiligde internetcommunicatie via web browsers zou moeten garanderen, maar waarvan de beveiliging in de praktijk meerdere malen is doorbroken. Tijdens het DigiNotar-incident in 2011, bijvoorbeeld, werd de Gmail-communicatie van 300.000 Iraanse IP-adressen onderschept en kon de veiligheid van internetcommunicatie in Nederland een week lang niet gegarandeerd worden. Het incident resulteerde in een mogelijk verlies van levens van Iraanse activisten en een geraamde schade van € 250 miljoen voor de Nederlandse economie. Ook al zijn deze incidenten breed uitgemaait in de media en jarenlang besproken in (inter)nationale politieke en bestuurlijke fora, blijven de onderliggende systematische kwetsbaarheden tot op de dag van vandaag grotendeels onopgelost.

Tegen de achtergrond van onze toenemende afhankelijkheid en ons groeiende bewustzijn dat privé-communicatie systematisch kwetsbaar is, onderzoekt deze studie de rol van de Europese Unie in het beschermen van
communicatiebeveiliging voor eindgebruikers. De studie combineert descriptief en normatief juridisch onderzoek, evenals onderzoeksmethoden uit de economische theorie en computer science, om de volgende centrale onderzoeksvraag te beantwoorden: *hoe zou de EU-wetgever de beveiliging van privé-communicatie moeten beschermen?*

Deel I van het proefschrift bevat een historische analyse van EU-wetgeving rondom communicatiebeveiliging gedurende de afgelopen 25 jaar. Daarmee presenteert deze studie het eerste uitgebreide overzicht in de juridische literatuur van het Europees regelgevend kader voor communicatiebeveiliging. Het proefschrift concludeert dat de EU zich, na medio jaren ’90 en ‘9/11’, in een ingrijpende derde reguleringsgolf bevindt rondom communicatiebeveiliging. Daarin onderscheidt de studie vijf ‘policy cycles’: i) netwerk- en informatiebeveiliging; ii) dataprotectie; iii) het Telecoms Package; iv) digitale certificaten, en v) cybercrime. Voor elke beleidscyclus beschrijft de studie de gebruikte definities van ‘veiligheid’, de reikwijdte, de belangrijkste maatregelen en de structuren voor toezicht. De studie identificeert vervolgens diepe conceptuele weeffouten en een lappendeken van bescherming voor eindgebruikers die dwars door de vijf beleidsterreinen loopt, en essentiële delen van hedendaagse waardeketens in de genetwerkte communicatieomgeving onbeschermd laat.

Met deze bevindingen ontwikkelt hoofdstuk 3 een analytisch kader voor het proefschrift, aan de hand van vier thema’s: i) ‘veiligheid’: conceptuele verwarring; ii) reikwijdte: ‘persoonsgegevens’ en actoren; iii) EU-recht, nationale veiligheid en communicatiebeveiliging, en iv) strategieën voor ‘veiligheid’: bescherming van netwerken en systemen vis-à-vis afschrikking van aanvallers.
Deel II van het proefschrift onderzoekt de concepten en instrumenten voor de bescherming van communicatiebeveiliging via EU-recht, vanuit het perspectief van de grondrechten (hoofdstuk 4), systeemontwerp (hoofdstuk 5) en de politieke wetenschap (hoofdstuk 6). Hoofdstuk 4 identificeert en ontwikkelt de positieve verplichtingen op basis van de grondrechten in het EU-verdrag voor de EU-wetgever om de beveiliging van privé-communicatie te garanderen. De nieuwe positieve verplichtingen hiertoe voor de EU-wetgever – zoals uiteengezet in de Digital Rights Ireland a.o. uitspraak van het Hof van Justitie van de EU dat de omstreden Europese dataretentierichtlijn nietig verklaarde – worden verder ontwikkeld door conceptuele en normatieve analyse. Het proefschrift beargumenteert onder andere dat communicatiebeveiliging een basisgarantie vormt tegen arbitraire inbreuken op andere fundamentele rechten, zoals privacy en communicatievrijheid, die op hun beurt essentieel zijn om een breed scala aan grondrechten te beschermen, zoals godsdienstvrijheid en de vrijheid van vereniging. Deel III, met name de casestudies over de Snowden-onthullingen, bouwt voor en concretiseert de normatieve conclusies van het grondrechtelijke perspectief op communicatiebeveiliging van hoofdstuk 4.

Hoofdstuk 5 onderzoekt de elementen van de technische definitie van ‘veiligheid’: vertrouwelijkheid, integriteit en beschikbaarheid (de zogenaamde c.i.a.-triad). Het hoofdstuk beschrijft ook leidende theorieën rondom systeemontwerp, zoals ‘Multilateral Security Requirements Analysis’, en waarom beveiliging in de praktijk zo vaak doorbroken wordt, waarbij de studie onderscheid maakt tussen falen door de gebruiker, de technologie, marktfalen en surveillance. De studie staat ook stil bij ‘security economics’. Deze snel aan invloed winnende wetenschapsrichting combineert inzichten uit de economische theorie met computer science, en neemt als uitgangspunt dat de kwakkelende beveiliging van informatie en communicatie veelal geen technische oorzaak heeft, maar te wijten valt aan een gebrek aan prikkels voor aanbieders in de markt om te investeren in beveiliging. Markten voor
beveiliging zijn ondoorzichtig, weinig concurrerend en eventuele schade bij doorbrekingen van beveiliging worden niet geleden door de aanbieders in de markt, die geen aansprakelijkheid hoeven aanvaarden, maar door de afnemer of eindgebruiker.

Hoofdstuk 6 verkent de politieke theorieën rondom veiligheidsbeleid en de politieke dynamiek rondom de bescherming van communicatiebeveiliging via EU-recht. De studie beschrijft de aanzienlijke conceptuele verschillen tussen de technische en politieke definities van ‘veiligheid’ en verbindt deze verschillen aan gevestigde theorieën zoals ‘securitization’ en de hedendaagse focus op subjectieve veiligheid in plaats van objectieve veiligheid. Dit politieke perspectief op de bescherming van privé-communicatie geeft meer inzicht in de laterale thema’s van de historische analyse, zoals de aanhoudende gijzeling van EU-wetgeving door nationale veiligheids- en de economische belangen in de afgelopen 25 jaar, alsmede de focus op afschrikking van cybervaanvallen, in plaats van het het realiseren van de vertrouwelijkheid, integriteit en beschikbaarheid van genetwerkte communicatie via EU-wetgeving.

Deel III van de studie bouwt voort op de analyse van Deel II en ontwikkelt een nieuw model voor de stapsgewijze analyse of, en zo ja, hoe de EU-wetgever privé-communicatiebeveiliging zou moeten beschermen. Dit model, uiteengezet in hoofdstuk 7, bestaat uit de volgende zes stappen:

1. Breng de functionele waardeketen van de onderzochte communicatiesetting in kaart;
2. Identificeer systematische kwetsbaarheden;
3. Analyseer bestaande surveillance- en marktprikkels;
4. Operationaliseer de ‘c.i.a.-triad’ en de fundamentele rechten;
5. Onderzoek bestaande technische oplossingen;

Hoofdstuk 9 onderzoekt communicatiebeveiliging in de ‘cloud’ door de lens van de Snowden-onthullingen, in het bijzonder operatie MUSCULAR. Met operatie MUSCULAR onderschepten Amerikaanse en Britse inlichtingendiensten onvoorstelbare hoeveelheden privé-communicatie van tientallen miljoenen eindgebruikers, bijvoorbeeld tussen Google’s en Yahoo’s datacenters, zonder dat de ‘cloud’ aanbieders hiervan op de hoogte waren gesteld. Omdat deze aanbieders stilaan begonnen met het bieden van communicatiebeveiliging in hun directe communicatieketens met gebruikers – bijvoorbeeld via HTTPS in webbrowsers – verlegden de inlichtingendiensten hun surveillance naar de interne netwerken van de providers. Intern en onderling communiceerden de aanbieders de data van eindgebruikers namelijk zonder additionele beschermingsmaatregelen. De casestudie concludeerde onder andere dat de bescherming van privé-communicatie moet worden uitgebreid tot de gehele functionele waardeketen van elektronische communicatie (‘end-to-end’) en dat het providers, nu de ophef rondom MUSCULAR is weggezet, nog steeds aan marktprikkels ontbreekt om privé-
communicatie en fundamentele rechten van eindgebruikers in de ‘cloud’ daadwerkelijk te beschermen.

Deel IV beantwoordt de centrale onderzoeksvraag van het proefschrift. De EU-wetgever, concludeert deze studie, integreert cruciale grondrechtelijke-, sociaal-technische- en marktontwikkelingen onvoldoende in EU-wetgeving. Het proefschrift biedt vijf brede aanbevelingen voor de EU-wetgever om privé-communicatiebeveiliging te beschermen:

1. De EU-wetgever moet de uit de fundamentele rechten voortvloeiende positieve verplichtingen rondom privé-communicatiebeveiliging steviger veiligstellen in EU-wetgeving;
2. De impliciete en verborgen gijzeling van EU-wetgeving door nationale veiligheidsbelangen van de lidstaten moet in de toekomst geëxpliciteerd en genuanceerd worden;
3. De EU-wetgever dient bescherming te bieden in de gehele functionele waardeketen van elektronische communicatie, in plaats van alleen aan ‘persoonsgegevens’ of ten aanzien van conventionele telecom-aanbieders, zoals internet access providers.
4. De EU-wetgever zou hardnekkig marktfalen in communicatiebeveiliging moeten aanpakken;
5. Het analytische model van Deel III biedt een nieuw vertrekpunt voor de bescherming van privé-communicatiebeveiliging in EU-wetgeving.

Ten slotte schetst het proefschrift de vooruitzichten van de bescherming van privé-communicatiebeveiliging via EU-wetgeving op de korte en langere termijn. Zelfs na ernstige incidenten lijken de belangen voor de Europese Unie om privé-communicatie betekenisvol te beveiligingen te ontbreken. Echter, recente ontwikkelingen op grondrechtelijk en socio-technisch niveau – met name een aantal zorgwekkende veiligheidsincidenten rondom het ‘internet der dingen’ die onze fysieke veiligheid in gevaar brengen, bijvoorbeeld in de auto-
industrie – kunnen hernieuwd momentum creëren voor de in deze studie bepleite fundamentele herziening van het EU-recht rondom communicatiebeveiliging. Als de EU-wetgever de eerste vier aanbevelingen van het proefschrift niet integreert, zal de huidige derde reguleringsgolf van de EU rondom de beveiliging van onze privé-communicatie de conceptuele weefknoten van het verleden herhalen, de systematische kwetsbaarheden in de elektronische communicatieomgeving niet adresseren en de fundamentele rechten van Europeanen onvoldoende beschermen.
Acknowledgements

It’s been an exciting, frustrating, joyful, depressing, fascinating ride. Even if some still doubt whether we live in the Matrix or a world already overtaken by AI Superintelligence, after finishing this book I can safely establish that I’m not a robot. One of the implications of this perhaps unsurprising, yet existential finding, is that all the people that helped the project materialize did so with friendly advice, backup during rough times and essential tools for procrastination – rather than commands. I can’t even begin to name all the family, friends and colleagues who made this project happen, and make life generally worth it’s while. For the print edition of the thesis, I’ll promise to once again stare at all the world’s cognitive tools and try, yet again, to comprehensively list all of you. I would probably need an extra 5 sheets of paper. Now, for this ‘academic version’ that I will soon submit to the Office of the Beadle to comply with University regulations, I must hand in 12 books. Consequently, listing all of you would probably add up to some 60 extra pages printed out of the University’s non-eco printer, on non-sustainable paper. That adds up to about 0.1% percent of a tree. So for now, rather than my incompetence at writing acknowledgements, let’s blame it on the environment. Anyway, profound thanks to all of you – you know who you are.

A few data subjects deserve special thanks. Nico van Eijk and Bernt Hugenholtz, directors of the Institute for Information Law (IViR) at the time, and Edgar du Perron, Dean of the Law Faculty at the University of Amsterdam, thanks for handing me a four-year carte blanche to explore this new direction in information law. Nico van Eijk and Natali Helberger, my supervisors, thanks for your inspiration, support and pressing the kill switch at vital moments when I sought to take the project in yet again a new direction. The freedom, intellectual space and financial backup we enjoy at IViR is truly special.
Thanks to Urs Gasser, Rebecca Tabasky, Edward Felten and Steve Schultze for inviting me to become a Fellow at Harvard’s Berkman Center for Internet & Society and Princeton’s Center for Information Policy during the 2013-14 academic year. Stichting Democratie & Media, Prins Bernhard Cultuurfonds and Stichting Internet4ALL, thank you for the financial support. Helen Nissenbaum and Bernardo Innocenti and the Sacramento place crowd, thanks for having me over at your wonderful homes in Princeton and Cambridge, MA.

To all my co-authors – Hadi Asghari, Frederik Borgesius, Michel van Eeten, Sharon Goldberg, Joris van Hoboken, and Nico – thank you for your insights and willingness to trade sleep for frantic writing, always against the clock. Over a beer, or perhaps four in Brussels after a conference in 2010, the late Caspar Bowden convinced me to start digging into the Patriot Act and FISA. Boy, does Casper keep on rocking. Chris Hoofnagle introduced me to US academia and taught me a lesson or two about finding your way in the maze. Joris and Seda Gürses, thanks for your insights and the lolz, as goes for Ian Brown, Chris Soghoian, Joe McNamee, Ashkan Soltani, Primavera de Filippi, Maxime Lambrecht, Bruce Schneier, Bill Binney, Diego Vicentin, Josh Kroll, Peter Eckersley, the Berkman Fellows and the β0ɛk3nc17π.

Frederik, the book benefits enormously from your painstakingly precise feedback and all the fun we had. I still don’t understand the peculiar decision to put the two most easily distracted, bouncy and noisy colleagues in a tiny room on the first floor. Actually, re-reading that last sentence, I finally do. Ot van Daalen, thanks for everything you taught me about technology, writing, sticking to a strategy, getting things done and the integrity you bring to the table. Reminds me of my dad. And Welmoed, since the medium is the message, I'll only use my thesis as a proxy server to broadcast publicly that your soul is deeply embedded in these pages. For the details, I know we’re both perfectly happy to resort to secure, private communications in the privacy of our home.