



UvA-DARE (Digital Academic Repository)

Surveillance as public matter

Revisiting sousveillance through devices and leaks

van der Velden, L.C.

Publication date

2018

Document Version

Other version

License

Other

[Link to publication](#)

Citation for published version (APA):

van der Velden, L. C. (2018). *Surveillance as public matter: Revisiting sousveillance through devices and leaks*. [Thesis, fully internal, Universiteit van Amsterdam].

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: <https://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.

Summary

Surveillance as public matter:

Revisiting sousveillance through devices and leaks

Concepts of surveillance have not kept pace with digital innovations. Therefore, projects that render (digital) surveillance visible and knowable become interesting analytic starting points. Since surveillance consists of technical and often secret processes, this 'rendering visible' inevitably requires a form of translation. This translation process is the main concern of this thesis: How is surveillance made public? It tackles this question by combining an empirical inquiry on how surveillance is traced, made visible and understandable with a conceptual search for new vocabularies to address surveillance practices and countermeasures.

In the first chapter, "Tackling internet surveillance", I introduce this main concern by situating the issue of surveillance within critical internet cultures. Media theorists and anthropologists have stressed that interventions with media technologies are key to the critical internet scene and hacker cultures, that freedom of information and openness are important points of reference, and that network cultures provide (experimental) settings from which particular methods and approaches are emerging. Also seen from this body of practices, surveillance is a well-known object of intervention. It is something that can be intervened with by technical interrogation and exposure.

I then discuss how Surveillance Studies have tackled surveillance conceptually with a dedicated concept for exposing surveillance, which is the notion of 'sousveillance'. 'Sousveillance' is usually associated with inversed surveillance in which people monitor the authorities. It is this particular niche within Surveillance Studies to which my work connects, but my study emphasises different aspects of sousveillance than the ones usually highlighted in the sousveillance literature. Instead of looking at the reflexive effects of encounters by which the watchers are being watched, I propose to focus on instruments and methods for bringing surveillance into view. After discussing sousveillance I demarcate a specific conceptual trajectory within Surveillance Studies that calls for new conceptualisations in response to new digital technologies and which moves towards assemblage-oriented theory in which (surveillance) agency is more evenly distributed than centrally

organised. This thesis is coherent with that tradition in so far as it takes into consideration the possibility that different technologies require different conceptual registers, and that assemblages require a particular research focus.

In the second chapter, I make the argument that it is useful to bring Surveillance Studies into conversation with Actor Network Theory (ANT) to guide this conceptual revision. ANT is an approach that can be described as a material-semiotic reading of techno and scientific practices. I discuss several 'reluctant accounts' of ANT by summarising authors that do not present ANT as a method with straightforward instructions, but take a detour in explaining the approach. In doing that, they 'make space'. Latour presents a negative method of ANT, making space for the voices of the actors. Law presents an account in translation, making space for variations that contributors add to ANT. Mol presents a repository of sensitive terms, making space for a dynamics of changing things. I use the suggestions of these authors to update the conceptual repertoire around surveillance and sousveillance in a way that follows the movements and translations made by the actors.

In the analysis, the notion of the 'device', central to ANT, is important. The device denotes the interactive process between human and non-human constituents that allow for action to emerge. Since the device is an operator of translations, it gives guidance to not only the distribution of action, but more importantly, the reorganisation of action. From device-centred modes of thinking I draw especially on literature that stresses the material dimensions of contemporary publics, which means that special attention is given to the active role of devices and material artefacts in shaping how publics and public problems are organised and articulated. I argue that notions of 'material publics' are particularly useful to think about interventions with and exposures of surveillance because rendering (digital) surveillance visible obviously requires a form of translation. In this translation, devices can play a formative role. Mobilising notions of material publics for surveillance studies allows me to not only show some of the material dimensions of how surveillance is made public as 'visible' but also explain how surveillance is re-appropriated.

Against this context I put forward four case studies into four projects that make surveillance public, ranging from devices such as counter tracking applications for mobile phones and web browsing (*InformaCam* and *Ghostery*) to leaks of surveillance repositories (*WikiLeaks* and the *NSA disclosures*). I analyse these interventions through the notion of the socio-technical 'device', with a sensitivity to the materiality of publics. Empirically this means that I focus on the instruments through which surveillance is brought to the fore, the

transformations that take place along that trajectory, the importance of the different settings in which this happens, and the kinds of publics these configurations (could) enact. Conceptually I aim to use a conceptual vocabulary that is fitting to the specificity of these cases.

Each chapter presents an ‘ANT-story’ (Law 1997). Chapter three presents a story about about *making networks hold*. I analyse InformaCam as a ‘socio-technical device’ and show the translations that it makes. Chapter four is about *the performativity of devices*. I discuss how devices (in the case of the leaked datasets of WikiLeaks) can shape how data are ‘witnessed’. Chapter five, on Ghostery, is an *ANT inspired digital methods* study. I combine an analysis of a social-technical device with a personal research project: I move towards doing research into online tracking by ‘repurposing’ a surveillance awareness device. Finally, in chapter six I reflect upon the implications of the NSA affair for surveillance theory by trying to *develop an infra-language* (Latour 2005b) that reflects upon the consequences of their public presence.

Chapter three, “A forensic device for activism”, is an inquiry into the ‘laboratory’ of sousveillance practitioners. In this chapter, I propose that InformaCam should be interpreted as a ‘forensic device’. By using the conceptualisation of forensics (Weizman et al. 2010) and work on devices of demonstration (Barry 1999; Callon 2004) I show how InformaCam, through a range of interventions, establishes a translation: it re-arranges metadata into a technology of evidence. By treating data in this particular way, this app does more than enforcing awareness about surveillance. It becomes engaged with investigatory practices. My analysis shows that InformaCam indicates something significant for narratives about sousveillance, namely that singular acts of exposing the behaviour of authorities is only one part of the story. Instead of being concerned with what can be seen (on an image), the project shows how attention shifts to the ‘art’ of looking, which is concerned with how to organise which data counts.

Chapter four, “Transparency devices for leaked data”, presents a study on WikiLeaks. In the parlance of sousveillance theory, WikiLeaks is a form of ‘undersight’ (Van Buuren 2013). Others have said WikiLeaks carried a promise of ‘radical transparency’ (Birchall 2014; Heemsbergen 2014). I focus on working practices of ‘dealing with surveillance data’ in the context of leaking and discuss how they contribute to a particular form of expertise. Evelyn Ruppert has coined the notion of the ‘data public’, implying that digital devices reconfigure the production of expertise and play a constitutive role in how a public is enacted (Ruppert 2015). In this study I combine this insight with literature on WikiLeaks as a form of radical transparency (Birchall 2014) and reflect upon the role of tools and working practices around Wikileaks as an ‘unauthorised’ or ‘radical transparency’ project. In

the chapter, I argue that WikiLeaks could be seen as an experiment in *radical expertise*. It is an experiment in unauthorised knowledge production that requires investigatory data subjects – experts - that need a particular form of data literacy.

In chapter five, “Turning a safety tool into a microscope”, I show how a ‘sousveillant device’ enables the study of surveillance also for other researchers, such as myself. The chapter presents empirical findings about online tracking and it reflects on this ‘embedded sousveillance research’. The key actor is the browser plugin Ghostery. Ghostery makes surveillance public by detecting online trackers, ranking and making them visible. But it does more than give people a warning: it also analyses the trackers. In this study, I show how those research activities make Ghostery a participant in doing surveillance studies. Marres (2012b) uses the term ‘material participation’ to point at the role that devices play in the distribution of problems. Along these lines, I argue that this particular device develops particular social-technical ways of dealing with web tracking as a contemporary problem, both on the level of understanding and on the level of channelling action. I analyse how Ghostery participated in two ways in defining surveillance. First, it operates as an *issue device*, through its way of defining and ranking trackers, and second, as a *research device*, as a material research agent for conducting analysis of web tracking on governmental websites. By building upon work of the Digital Methods Initiative (DMI), which specialises in repurposing web devices for research (Rogers 2009b), I use a tool that is built on top of Ghostery, the ‘Tracker Tracker’, to map trackers on Dutch governmental websites. In this way, I conclude that Ghostery, by making web tracking mechanisms empirically and conceptually contributes to a particular understanding of contemporary consumer surveillance.

Chapter six, “Leaky apps and data shots”, returns to one of the central themes in the first chapter of the thesis: the reconceptualisation of notions of surveillance as a response to the introduction of new technologies. The NSA disclosures have brought specific surveillance devices into circulation, and the case study offers a reflection upon the consequences of that event. The central focus is on displaying a range of surveillance technologies that came to the fore through the disclosure of the NSA files in 2013. In this chapter, I briefly sketch how surveillance theory in the past has accommodated novel information and communication technologies and how, in the contemporary situation, the NSA files have lead to discussions, between academics and in public forums, about how contemporary surveillance society should be understood. By drawing on a set of news publications about the NSA files, I highlight two ways in which the NSA, or occasionally the GCHQ, captures data. The first consists of a list of programs that

extract data due to the fact that internet devices ‘leak’ data. The second is a list of devices that ‘insert’, for instance, malware. This is done in order to conceptualise two distinct forms of movement, leakage and insertion, by which data are captured by these intelligence agencies. It is an attempt to draw theoretical consequences from the presence of intelligence technologies in the public domain, and sketch a different imagination about surveillance by investigating the characteristics of the devices that the NSA documents present us with. Inspired by the works of Wendy Chun (2013) and Jussi Parikka (2007), I discuss the (theoretical) questions for each form and conclude by pointing out future sites of research for surveillance studies.

In chapter seven, “The materiality of surveillance made public”, the last and concluding chapter, I revisit the way I operationalised the question of how surveillance is made public and present the main conclusion of the dissertation. The conclusion can be reduced to the following three contributions. Firstly, contributing to Surveillance Studies, and in particular to the study of sousveillance assemblages, this study shows that sousveillance has a research dimension: surveillance is datafied and analysed. Secondly, by incorporating insights into the formation of material publics, it shows that the analytic styles by which this happens are embedded in particular working environments. In tackling surveillance, projects produce surveillance data. Since there is a diversity of working styles through which surveillance is data are produced and disclosed, surveillance is to be taken up in diverse configurations of understanding. Thirdly, bridging Surveillance Studies and literature on material publics within Science and Technology Studies, I conclude that the examples demonstrate how surveillance can become ‘public matter’: in the process of turning surveillance into a matter of concern, surveillance becomes ‘datafied’ itself and this material can be used for public ends. The devices transform data monitoring technologies into online tools for forensics and research; the leaks become input for radical data literacy and open up new research trajectories: surveillance-material, taking on the shape of a public archive, puts surveillance theory under pressure.

Resonating with how critical internet culture treats other forms of online material (and code), surveillance is turned into public working material. Surveillance as public matter should express the empirical insight that surveillance is turned into public resource for re-appropriation. Making public is therefore also making public for future and collective use, and possibly for tactical use. The notion of ‘making public’, being one that is borrowed from the Latourian exhibition and publication about the ‘politics of things’ (Latour and Weibel 2005), also signals that this transformation is bound to those that shape it into a matter of concern.

At the end of the concluding chapter, I reflect upon the implications of the thesis. It opens a future research agenda into 'surveillance publics'. These are publics that are situated in a socio-technical environment in which intelligence, secrecy and privacy practices co-determine the modes of working, and thus, interestingly, 'making private' coincides with ways of making public. Finally, since surveillance awareness interventions open up surveillance as material for research, the dissertation calls for more collaboration between academics and technical (sometimes radical) experts and for supporting infrastructures to allow this to happen.

Nederlandse samenvatting

Surveillance als publieke materie:

Een herziening van sousveillance in het licht van digitale apparaten en gelekte data.

Theorieën over surveillance kunnen de snelle digitale ontwikkelingen maar nauwelijks bijbenen. Daarom zijn projecten die digitale surveillance zichtbaar en inzichtelijk maken interessant als startpunten voor het formuleren van nieuwe begrippen. Omdat digitale surveillance bestaat uit technische (en vaak geheime) processen, maken dit soort projecten noodzakelijkerwijs een vertaalslag. Dergelijke vertaalslagen (ofwel 'translaties') staan centraal in dit proefschrift: Hoe wordt surveillance publiek gemaakt? Het proefschrift gaat in op deze vraag, door empirisch onderzoek te combineren met een zoektocht naar een nieuw vocabulaire voor het adresseren van surveillance en eventuele tegenmaatregelen.

In het eerste hoofdstuk, "Tackling surveillance", introduceer ik deze kwestie, door het onderwerp van surveillance te situeren binnen kritische internetculturen. Mediatheoretici en antropologen hebben laten zien dat interventies met nieuwe media een centrale activiteit vormen binnen zogeheten de kritische internetscene en hackerculturen, dat de vrije circulatie van informatie een centraal referentiepunt vormt, en dat netwerkculturen de (experimentele) condities vormen voor het ontstaan van specifieke methoden en benaderingen. Binnen dit geheel aan praktijken, is surveillance een bekend object, dat technisch ondervraagd en blootgelegd wordt.

Vervolgens bespreek ik hoe het veld Surveillance Studies surveillance conceptueel gezien 'getackeld' heeft, middels het concept 'sousveillance'. Sousveillance verwijst naar 'omgekeerde surveillance' waarbij mensen de surveillance-apparatuur (terug)richten naar de autoriteiten. Mijn werk is relateerd aan dit specifieke deelgebied binnen Surveillance Studies, maar belicht een andere dimensie dan doorgaans wordt aangekaard via de sousveillance literatuur. Analyses van sousveillance wijzen doorgaans op de reflectieve interrupties die deze interventies veroorzaken. Dit proefschrift staat een andere benadering voor door expliciet te willen kijken naar de instrumenten en methodes waarmee surveillance zichtbaar wordt gemaakt. Het benadert praktijken van sousveillance als praktijken van kennisproductie. Vervolgens

sluit ik me aan bij denkers binnen de Surveillance Studies die pleiten voor een herziening van concepten van surveillance als reactie op digitale transformaties, en een beweging hebben gemaakt richting een begrippenkader dat spreekt in termen van assemblages. Zij zien het handelingsvermogen van surveillance actoren en technologieën niet als een gecentraliseerd 'Big Brother-achtig' fenomeen, maar als een gedistribueerd proces. Dit proefschrift volgt hun stellingname in zoverre dat het in oogschouw neemt dat verschillende technieken verschillende conceptuele registers aanspreken, en dat assemblages om een specifieke onderzoeksfocus vragen.

In hoofdstuk twee, "Devices for making surveillance public", breng ik Surveillance Studies in dialoog met Actor Network Theorie (ANT) om deze conceptuele herziening te begeleiden. ANT is ook wel bekend als een materiële semiotiek van wetenschappelijke en technologische praktijken. Ik bespreek drie beschrijvingen van ANT die wat 'onwillig' geformuleerd zijn: zij presenteren geen eenduidig verhaal over ANT met kant-en-klare instructies, maar maken daardoor wel analytische ruimte vrij. Latour presenteert een zogenaamde 'negatieve methode', waardoor ruimte wordt gemaakt voor de taal en bijdrage van de actoren onder studie. Law presenteert ANT als een 'verhaal in vertaling', waardoor er ruimte is voor onderzoekers om veranderingen aan te brengen aan het verhaal dat ANT vormt. Mol presenteert ANT als een 'flexibel repertoire van sensitieve termen', waardoor ruimte komt voor een dynamiek van veranderende dingen. Ik gebruik deze aanwijzingen om het conceptuele repertoire rondom surveillance en sousveillance te updaten op een manier dat concepten zich voegen naar de bewegingen en veranderingen van de actoren.

In de analyse neemt het concept van het 'socio-technisch apparaat' (*socio-technical device*), een belangrijk begrip in ANT, een centrale rol in. Dat begrip articuleert het idee dat menselijke en niet-menselijke onderdelen in samenspel handelen en middels een vertaalslag nieuwe handelingen mogelijk maken. Daardoor is het begrip niet alleen zinnig om kwesties van gedistribueerdheid te beschrijven, wat de Surveillance Studies reeds hebben gedaan, maar met name om het ook reorganiseren van handelingsmogelijkheden te duiden. Uit het geheel van literatuur dat een dergelijke notie van het apparaat hanteert, borduur ik met name voort op werk dat focust op de materiële dimensies van hedendaagse publieken. Dat wil zeggen dat binnen deze benaderingen bijzondere aandacht is voor hoe technieken (apparaten) een actieve rol spelen in de totstandkoming en articulatie van publieken.

Dit laatste doe ik omdat noties van materiële publieken met name relevant zijn om interventies met betrekking tot surveillance netwerken te doordenken. Dit is met name zo omdat de vertaalslag waarbij surveillance zichtbaar wordt gemaakt (digitale) technieken een

formatieve rol spelen. Het inzetten van noties van materiële publieken in Surveillance Studies maakt het niet alleen mogelijk in te zien wat het technisch en materieel gezien omvat om surveillance zichtbaar te maken, maar ook hoe activisten zich surveillance kunnen toe-eigenen.

Tegen deze achtergrond breng ik vier case studies naar voren die duidelijk maken hoe surveillance publiek wordt gemaakt. De gekozen voorbeelden variëren van mobiele en online applicaties die tracking detecteren en verhinderen (InformaCam en Ghostery), tot bekende lekken van documenten over surveillance (publicaties van WikiLeaks en de NSA-onthullingen). Ik analyseer deze interventies met behulp van de notie van het socio-technische ‘apparaat’, en met speciale aandacht voor de materialiteit van publieken. Dit betekent empirisch gezien dat ik focus op de instrumenten waarmee surveillance zichtbaar wordt gemaakt, de transformaties die daardoor plaatsvinden, het belang van de verschillende settings waarin dit gebeurt, en het soort publieken dat deze configuraties met zich mee (kunnen) brengen. Conceptueel gezien gebruik ik een vocabulair dat past bij de specificiteit van de verschillende casus.

Hoofdstuk drie, “A forensic device for activism”, is een onderzoek naar wat je het ‘laboratorium’ van de sousveillance beoefenaars zou kunnen noemen. In dit hoofdstuk bespreek ik InformaCam, een voorloper van een applicatie die mensen bewust maakt van metadata in beeldmateriaal en het mogelijk maakt om metadata op een specifieke manier te beheren. Door metadata op een bepaalde manier te behandelen, is de applicatie meer dan een manier om mensen bewust te maken van metadata, maar krijgt het tevens een opsporende functie in de context van mensenrechtenschendingen. Daarom beargumenteer ik dat de applicatie InformaCam beschouwd kan worden als een ‘forensisch apparaat’. Met behulp van het concept *forensics* (Weizman et al. 2010) en studies naar demonstraties (Barry 1999; Callon 2004) laat ik zien hoe InformaCam middels een aantal interventies een vertaalslag teweegbrengt: het reorganiseert metadata tot een techniek van bewijsvoering. Die analyse laat zien dat InformaCam bestaande interpretaties over sousveillance overstijgt. Het gaat niet alleen om de visuele dimensie en het blootleggen van het gedrag van autoriteiten. Dat is slechts een deel van het verhaal. In plaats van wat beeldmateriaal laat zien, wordt de ‘kunst’ van het kijken van belang: namelijk de organisatie van welke data telt.

Het vierde hoofdstuk, “Transparency devices for leaked data”, presenteert een analyse van WikiLeaks. Sommigen binnen de sousveillance theorie beschouwen WikiLeaks als klokkenluidersplatform dat ‘undersight’ inzet (Van Buuren 2013). Anderen bespeurden in WikiLeaks een belofte van ‘radicale transparantie’ (Birchall 2014; Heemsbergen 2014). Dit hoofdstuk gaat over de verschillende

manieren van werken met surveillance-data in de context van gelekte gegevens, en hoe deze werkpraktijken bijdragen aan een bepaalde vorm van expertise. Ruppert heeft de notie van een ‘datapubliek’ geduid, waarmee ze bedoelt dat digitale technieken de productie van expertise reorganiseren en mede bepalen hoe een publiek tot stand komt (Ruppert 2015). Het hoofdstuk combineert dit inzicht met literatuur over WikiLeaks als een vorm van radicale transparantie en reflecteert op de rol van technieken en werkpraktijken rondom WikiLeaks als een ongeautoriseerd of radicaal transparantieproject. In het hoofdstuk beargumenteer ik dat WikiLeaks gezien kan worden als een experiment in radicale expertise. Het is een experiment met ongeautoriseerde kennisproductie dat behoefte heeft aan onderzoekende data-subjecten (experts) die een specifieke vorm van data-geletterdheid onder de knie hebben of kunnen krijgen.

In hoofdstuk vijf, “Turning a safety tool into a microscope”, laat ik zien hoe een ‘sousveillance apparaat’ onderzoek ontsluit naar surveillance, ook voor onderzoekers zoals mijzelf. Het hoofdstuk presenteert empirische resultaten naar online tracking en het reflecteert op dit ‘ingebod’ sousveillance onderzoek. De centrale actor in het hoofdstuk is Ghostery, een browser plugin. Ghostery maakt surveillance publiek door online trackers te detecteren, te rangschikken en zichtbaar te maken. Naast waarschuwingen voor online tracking, biedt Ghostery ook een analyse van dit fenomeen. In het hoofdstuk laat ik zien hoe Ghostery deelneemt aan surveillance studies. Marres (2012b) gebruikt de term ‘materiële participatie’ om te duiden op de rol die apparaten spelen in de distributie van problemen. In lijn hiermee beargumenteer ik dat dit specifieke apparaat gekenmerkt wordt door een bepaalde socio-technische manier van omgaan met web tracking als hedendaags probleem. Ik analyseer vervolgens hoe Ghostery op twee manieren deelneemt in het definiëren van surveillance: Ten eerste als een *issue device*, door de manier waarop het trackers definieert en rangschikt, brengt het een bepaalde definitie van de kwestie consumentensurveillance naar voren. Ten tweede, als *research device*, een materiële onderzoekspartner om een concrete analyse uit te voeren op een dataset van overheidswebsites. Door voort te bouwen op het werk van het *Digital Methods Initiative (DMI)*, gespecialiseerd in het hergebruiken van web technieken (*web devices*) voor onderzoeksdoeleinden (Rogers 2009b), gebruik ik een tool die het DMI gebouwd heeft op basis van de detectietechnieken van Ghostery: de Tracker Tracker. De Tracker Tracker maakt het mogelijk om trackers zichtbaar te maken op overheidswebsites en onderlinge relaties tussen trackers en websites te verkennen. In mijn case studie heeft de tool laten zien dat de websites van de Rijksoverheid voor een groot gedeelte deelnemen aan de data-economie op een manier waar grote

bedrijven profijt van hebben. Op deze twee manieren draagt Ghostery zowel conceptueel als empirisch bij aan inzichten in hedendaagse consumentensurveillance.

Hoofdstuk zes, “Leaky apps and data shots” keert terug naar een van de hoofdthema’s in het eerste hoofdstuk: de herconceptualisering van begrippen van surveillance als respons op de introductie van nieuwe technologieën. De NSA-onthullingen in 2013 hebben kennis over specifieke surveillance-apparaten in circulatie gebracht. Dit hoofdstuk reflecteert op de gevolgen daarvan. De nadruk ligt op het tonen van een reeks aan surveillancetechnieken die naar voren kwamen in de onthullingen. In het hoofdstuk schets ik kort hoe surveillancetheorie nieuwe digitale technieken heeft geacommodeerd en hoe de NSA-documenten geleid hebben tot discussies, zowel tussen academici als in publieke fora, over hoe de hedendaagse surveillancesamenleving begrepen moet worden. Door gebruik te maken van een set aan nieuwpublicaties over de NSA-documenten, benadruk ik twee manieren waarop de Amerikaanse NSA, en soms ook de Britse GCHQ, data vergaren. Ten eerste via programma’s die data kunnen extraheren dankzij het feit dat veel van onze apparaten data ‘lekker’ (*leakage*). Ten tweede via technieken die zich als het ware ‘invogen’ (*insertion*) in computers of netwerken, zoals malware. Dit doe ik om twee verschillende ‘datavangende bewegingen’ te kunnen conceptualiseren. Het is een poging om theoretische consequenties te trekken van de aanwezigheid van surveillancetechnieken in het publieke domein, en een andere verbeelding van surveillance te schetsen door de kenmerken van de technieken serieus te nemen. Geïnspireerd door het werk van Wendy Chun (2013) en Jussi Parikka (2007) bediscussieer ik de (theoretische) vragen die iedere vorm opwerpt en concludeer ik door te wijzen op toekomstige onderzoeksgebieden voor studies naar surveillance en publieken in de context van surveillance.

In het concluderende hoofdstuk zeven, “The materiality of surveillance made public”, kom ik terug op de manier waarop ik de vraag ‘Hoe wordt surveillance publiek gemaakt?’ geoperationaliseerd heb. De conclusie van het proefschrift kan onderverdeeld worden in de volgende drie bijdragen aan de bestaande literatuur. Ten eerste, het draagt bij aan de Surveillance Studies, en met name het deelgebied van de studie naar *sousveillance assemblages*, door te laten zien dat *sousveillance* een onderzoeksdimensie heeft: door interventies die surveillance publiek maken wordt surveillance ‘gedataficeerd’ en geanalyseerd. Ten tweede, de werkwijzen waarmee dit gebeurt zijn ingebed in specifieke omgevingen. Door het onder handen nemen van surveillance, produceren *sousveillance* interventies diverse surveillance data. Aangezien er een diversiteit is aan werkstijlen waarmee data over surveillance wordt geproduceerd en blootgelegd, wordt surveillance als

kwestie opgenomen in verschillende begripsconfiguraties. Ten derde, middels een poging om Surveillance Studies te koppelen aan concepten van materiële publieken binnen de Wetenschap en Technologie Studies, concludeer ik dat het proefschrift laat zien hoe surveillance tot 'publieke materie' verwordt: in de vertaalslag van surveillance naar een publieke kwestie, verwordt surveillance zelf tot data, data die gebruikt kunnen worden voor publieke doeleinden. De detectie-apparaten die ik in dit proefschrift bespreek transformeren tracking technieken naar instrumenten voor forensisch werk en onderzoek; het gelekte materiaal wordt input voor radicale vormen van geletterdheid en opent nieuwe onderzoeksgebieden: in de vorm van een publiek archief, zet surveillance-materiaal bestaande surveillancetheorie onder druk.

Vergelijkbaar met andere praktijken in de kritische internetcultuur, waarin veel online materiaal wordt behandeld als publiek werkdomein (denk aan publieke code en licenties daarvoor), zien we dat surveillance eenzelfde transformatie of 'hack' doormaakt: het wordt publiek materiaal dat bewerkt en herschikt kan worden. 'Surveillance als publieke materie' moet uitdrukken dat surveillance tot publiek relevant onderzoeksmateriaal wordt gemaakt, een publieke bron die kan worden hergebruikt. Surveillance publiek maken is daarom ook publiek maken voor toekomstig en collectief gebruik, en mogelijk ook voor tactische doeleinden. Tegelijkertijd moet de term, refererend naar de notie van 'public matter' in Latour's Dingpolitiek, aangeven dat deze transformatie gebonden is aan de termen van degenen die haar tot publieke zaak maken.

Aan het eind van het hoofdstuk reflecteer ik op de implicaties van de dissertatie. Het opent een onderzoeksagenda naar 'surveillance-publieken'. Dit zijn publieken die gesitueerd zijn in een socio-technische omgeving waarin intelligence, geheimhouding en privacypraktijken bepalend zijn voor de manier van werken. Vandaar vallen interventies van 'privéhouden' interessant genoeg vaak samen met strategieën van 'publiek maken'. Tenslotte, bij wijze van een meer 'materiële onderzoeksagenda' roept het proefschrift op om na te denken over de status en circulering van surveillance als teriaal, het verkennen van meer samenwerking tussen academici en technische (soms radicale) experts, en pleit het voor het ondersteunen van institutionele infrastructuren om dit mogelijk te maken.

References

Literature

- 30C3. 2013. "Opening Event mit Tim Pritlove." December, 30. Accessed August 9, 2016. https://www.youtube.com/watch?v=EY1VDXgu_M0.
- Adey, Peter. 2004. "Secured and Sorted Mobilities: Examples from the Airport." *Surveillance & Society* 1 (4): 500–519. <http://www.surveillance-and-society.org>.
- Albrechtslund, Anders. 2008. "Online Social Networking as Participatory Surveillance." *First Monday* 13 (3). <http://firstmonday.org/ojs/index.php/fm/article/view/2142>.
- Andrejevic, Mark. 2014. "Wikileaks, Surveillance and Transparency." *International Journal of Communication* 8 (0): 2619–2630. <http://ijoc.org/index.php/ijoc/article/view/2669/1241>.
- Apitz, Sabrina. 2015. "Why the Snowden Files Should Be Made Accessible through Public Libraries. A Position Paper." *Berliner Gazette: Kultur, Politik und Digitales – seit 1999*. November 13. Accessed October 27, 2017. <http://berlingazette.de/snowden-files-public-library-position-paper/>.
- Appelbaum, Jacob, Judith Horchert, and Christian Stöcker. 2013. "Catalog Reveals NSA Has Back Doors for Numerous Devices." *Spiegel Online*, December, 29. Accessed June 30, 2014. <http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html>.
- . 2014. *When Google Met WikiLeaks*. OR Books.
- . 2015. "Introduction." In *The WikiLeaks Files: The World According to US Empire*, edited by Wikileaks. London: Verso Books.
- Assange, Julian, Jacob Appelbaum, Andy Müller-Maguhn, and Jérémie Zimmermann. 2012. *Cypherpunks Freedom and the Future of the Internet*. OR Books.
- Bakir, Vian. 2009. "Tele-Technologies, Control, and Sousveillance: Saddam Hussein — De-Deification and the Beast." *Popular Communication* 7 (1): 7–16. doi:10.1080/15405700802584262.
- . 2010. *Sousveillance, Media and Strategic Political Communication: Iraq, USA, UK*. New York: Bloomsbury Academic.
- Bal, Roland. 2005. "How to Kill with a Ballpoint: Credibility in Dutch Forensic Science." *Science, Technology & Human Values* 30 (1): 52–75. doi:10.1177/0162243904270722.
- Ball, Kirstie. 2002. "Elements of Surveillance: A New Framework and Future Directions." *Information, Communication & Society* 5 (4): 573–590. doi:10.1080/13691180208538807.
- Ball, Kirstie, Kevin D. Haggerty, and David Lyon. 2012. "Introducing

- Surveillance Studies." In *International Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin Haggerty, and David Lyon. Oxon; New York: Routledge.
- Barry, Andrew. 1999. "Demonstrations: sites and sights of direct action." *Economy and Society*, 28(1), 75–94. doi: 10.1080/03085149900000025.
- . 2010. "Transparency as a political device." In *Débordements : Mélanges offerts à Michel Callon*, edited by Madeleine Akrich, Yannick Barthe, Fabian Muniesa, and Philippe Mustar, 21–39. Paris: Presses des Mines. <http://books.openedition.org/pressesmines/721>.
- . 2013. "The Translation Zone: Between Actor-Network Theory and International Relations." *Millennium - Journal of International Studies* 41 (3): 413–29. doi:10.1177/0305829813481007.
- Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8 (2): 121–44. doi: 10.1111/ips.12048.
- Beaulieu, Anne, Andrea Scharnhorst, and Paul Wouters. 2007. "Not Another Case Study A Middle-Range Interrogation of Ethnographic Case Studies in the Exploration of E-Science." *Science, Technology & Human Values* 32 (6): 672–92. doi:10.1177/0162243907306188.
- Benkler, Yochai. 2013. "WikiLeaks and the Networked Fourth Estate." In *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*, edited by Benedetta Brevini, Arne Hinz, and Patrick McCurdy, 11–34. London: Palgrave Macmillan UK.
- Bennett, Colin. 2011. "In Defense of Privacy: The Concept and the Regime." *Surveillance & Society* 8(4): 485– 496. <http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4184>
- Berger, Lynn. 2014. "Zo Kunnen We Beter over Surveillance Praten." *De Correspondent*. June 2. <https://decorrespondent.nl/1237/zo-kunnen-we-beter-over-surveillance-praten/41215603-67a22001>.
- Berry, David. 2014. "The Antinomies of Computation." Blog. *Stunlaw: philosophy and critique for a digital age*. April 4. Accessed June 30, 2014. <http://stunlaw.blogspot.nl/2014/04/the-antinomies-of-computation.html>.
- Bijker, Wiebe E. 1995. *Democratisering van de Technologische Cultuur. Inaugural Speech*. Voerendaal: Schrijen-Lippertz. [https://cris.maastrichtuniversity.nl/portal/en/publications/democratisering-van-de-technologische-cultuur\(e3d41278-6f12-4d0f-804d-8f955b3df3fe\).html](https://cris.maastrichtuniversity.nl/portal/en/publications/democratisering-van-de-technologische-cultuur(e3d41278-6f12-4d0f-804d-8f955b3df3fe).html).
- . 1997. *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change*. Cambridge, MA and London, England: MIT Press.
- . 2010. "How Is Technology made?—That Is the Question!" *Cambridge Journal of Economics* 34 (1): 63–76. doi:10.1093/cje/bep068.
- Birchall, Clare. 2014. "Radical Transparency?" *Cultural Studies & Critical Methodologies* 14 (1): 77–88. doi:10.1177/1532708613517442.
- Birkbak, Andreas. 2013. "From Networked Publics to Issue Publics:

- Reconsidering the Public/Private Distinction in Web Science." In *Proceedings of the 5th Annual ACM Web Science Conference*, 24–32. WebSci '13. New York, NY, USA: ACM. <https://doi.org/10.1145/2464464.2464489>.
- Boon, Floor, Deriz, Steven, Modderkolk, Huub. 2014. NSA Infected 50,000 Computer Networks with Malicious Software. *Nrc.nl*, November 23. Accessed June 27, 2014. <http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/>.
- Borra, Erik, and Bernard Rieder. 2014. "Programmed Method: Developing a Toolset for Capturing and Analyzing Tweets." *Aslib Journal of Information Management* 66 (3): 262–78. doi:10.1108/AJIM-09-2013-0094.
- Bowcott, Owen. 2015. "EyeWitness to Atrocities: The App Aimed at Bringing War Criminals to Justice." *The Guardian*, June 7, 2015. <http://www.theguardian.com/technology/2015/jun/08/eyewitness-to-atrocities-the-app-aimed-at-bringing-war-criminals-to-justice>.
- Bradshaw, Elizabeth. 2013. "This Is What a Police State Looks Like: Sousveillance, Direct Action and the Anti-Corporate Globalization Movement." *Critical Criminology* 21 (4): 447–61. doi:10.1007/s10612-013-9205-4.
- Brevini, Benedetta, Arne Hintz, and Patrick McCurdy, eds. 2013. *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*. London: Palgrave Macmillan UK. <http://link.springer.com/10.1057/9781137275745>.
- Brock, Jim. 2010. "Credibility Gap: What does Ghostery really see?" *Privacy Choice Blog*, March 4. Accessed January 25, 2014. <http://blog.privacychoice.org/2010/03/04/credibility-gap-what-does-ghostery-really-see/>
- Brooke, Heather. 2012. *The Revolution Will Be Digitised: Dispatches from the Information War*. London: Windmill Books.
- Brucato, Ben. 2015. "Policing Made Visible: Mobile Technologies and the Importance of Point of View." *Surveillance & Society* 13 (3/4): 455–73. <http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/point-of-view>.
- Cabledrum. 2013. Last modified September 27. <http://www.cabledrum.net/gifiles/>
- Callon, Michel. 1986. "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay." In *Power, Action and Belief: A New Sociology of Knowledge?*, 196–223. London: Routledge.
- . 2004. "Europe Wrestling with Technology." *Economy and Society* 33 (1): 121–34. doi:10.1080/0308514042000176766.
- Callon, Michel, and Fabian Muniesa. 2005. "Peripheral Vision Economic Markets as Calculative Collective Devices." *Organization Studies* 26 (8): 1229–50. doi:10.1177/0170840605056393.
- Caluya, Gilbert. 2010. "The Post-Panoptic Society? Reassessing Foucault in Surveillance Studies." *Social Identities* 16 (5): 621–33. doi:10.1080/13504630

.2010.509565.

- “CameraV app and the InformaCam System”. 2015. Last modified July 28. <https://guardianproject.github.io/informacam-guide/en/InformacamGuide.html>.
- Cardullo, Paolo. 2014. “Sniffing the City: Issues of Sousveillance in Inner City London.” *Visual Studies* 29 (3): 285–93. doi:10.1080/1472586X.2014.941550.
- Castronovo, Russ. 2013. “State Secrets: Ben Franklin and WikiLeaks.” *Critical Inquiry* 39 (3): 425–50. doi:10.1086/670040.
- Center for Research Libraries. 2012. “Human Rights Electronic Evidence Study: Final Report.” https://www.crl.edu/sites/default/files/d6/attachments/pages/HREES_Final_Report_Public.pdf.
- Chaos Computer Club. 2016. “33. Chaos Communication Congress: Wir bitten um Vortragseinreichungen.” August 31. Accessed October 3, 2017. <https://www.ccc.de/de/updates/2016/33C3-cfp>.
- Chokshi, Niraj. 2016. “Snowden and WikiLeaks Clash Over How to Disclose Secrets.” *The New York Times*, July 29. <https://www.nytimes.com/2016/07/30/us/snowden-wikileaks.html>.
- Chun, Wendy Hui Kyong. 2006. *Control and Freedom: Power and Paranoia in the Age on Fiber Optics*. Cambridge, MA: MIT Press.
- . 2013. *Wendy Hui Kyong Chun: Habitual New Media*. Barnard College in New York City, October 10. Accessed January 12, 2015. <http://vimeo.com/78287998>.
- Circumvention Tech Summit IV (CTS-IV). Organised by *Open ITP*. Berlin, September 29 - October 1, 2013. <http://openitp.org/openitp/circumvention-tech-summit.html>.
- Coleman, Gabriella. 2009. “CODE IS SPEECH: Legal Tinkering, Expertise, and Protest among Free and Open Source Software Developers.” *Cultural Anthropology* 24 (3): 420–454. doi:10.1111/j.1548-1360.2009.01036.x.
- . 2011. “Hacker Politics and Publics.” *Public Culture* 23 (3 65): 511–16. doi:10.1215/08992363-1336390.
- . 2012. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton and Oxford: Princeton University Press.
- Couldry, Nick, and Alison Powell. 2014. “Big Data from the Bottom up.” *Big Data & Society* 1 (2): 1–5. doi:10.1177/2053951714539277.
- Courage. 2015. “Announcement: Barrett Brown is Courage’s fifth beneficiary.” July 16. <https://couragefound.org/2015/07/announcement-barrett-brown-is-courages-fifth-beneficiary/>.
- Critical Art Ensemble. 1998. *Flesh Machine: Cyborgs, Designer Babies, & New Eugenic Consciousness*. New York: Autonomedia.
- Cult of the Death Cow. 2001. “The Hacktivism Declaration: assertions of liberty in support of an uncensored internet.” *cDc communications & HACKTIVISMO: “A Special Message of Hope*. July 4. Accessed October 3, 2017. http://www.cultdeadcow.com/cDc_files/declaration.html.
- Dean, Jodi. 2011. *Open 22. Transparantie. Openbaarheid En Geheimhouding in Het*

- Tijdperk van WikiLeaks*, edited by Jorinde Seijdel and Liesbeth Melis. NAI Uitgevers, SKOR. <https://www.naibooksellers.nl/open-22-transparantie-openbaarheid-en-geheimhouding-in-het-tijdperk-van-wikileaks.html>.
- De Haes, Andreas Udo. 2012. "Rijksoverheid zet alle cookies uit." *Webwereld*, August 9. <http://webwereld.nl/nieuws/111422/rijksoverheid-zet-alle-cookies-uit.html>.
- Deleuze, Gilles. 1992. "Postscript on the Societies of Control". *October* 59: 3–7.
- Deleuze, Gilles and Felix Guattari. 2009 [1987]. *A Thousand Plateaus: Capitalism and Schizophrenia*. London: Continuum.
- Dennis, Kingsley. 2008. "Viewpoint: Keeping a Close Watch– the Rise of Self-Surveillance and the Threat of Digital Exposure." *The Sociological Review* 56 (3): 347–57. doi:10.1111/j.1467-954X.2008.00793.x.
- De Souza e Silva, Adriana, and Jordan Frith. 2010. "Locational Privacy in Public Spaces: Media Discourses on Location-Aware Mobile Technologies." *Communication, Culture & Critique* 3 (4): 503–25.
- Deville, Joseph Edward, and Lonneke Van der Velden. 2015. "Seeing the Invisible Algorithm: The Practical Politics of Tracking the Credit Trackers." In *Algorithmic Life: Calculative Devices in the Age of Big Data*, edited by Louise Amoore and Volha Piotukh, 87–106. London: Routledge.
- De Vries, Gerard. 2007. "What Is Political in Sub-Politics? How Aristotle Might Help STS." *Social Studies of Science* 37 (5): 781–809. doi:10.1177/0306312706070749.
- De Winter, Brenno. 2012. "Overheidswebsites sturen gegevens door naar derden." *nu.nl*, November 1. <http://www.nu.nl/internet/2947863/overheidssites-sturen-gegevens-derden.html>.
- D'Ignazio, Catherine, Alexis Hope, Alexandra Metral, Ethan Zuckerman, David Raymond, Willow Brugh and Tal Achituv. 2016. "Towards a Feminist Hackathon: The 'Make the Breast Pump Not Suck!' Hackathon." *Journal of Peer Production* 8. <http://peerproduction.net/issues/issue-8-feminism-and-unhacking/peer-reviewed-papers/towards-a-feminist-hackathon-the-make-the-breast-pump-not-suck/>.
- Dijstelbloem, Huub. 2015. "Het Publieke Oog Als Privédetective." University of Amsterdam. <http://dare.uva.nl/record/1/473437>.
- Dijstelbloem, Huub, Albert Meijer, and Michiel Besters. 2011. "The Migration Machine." In *Migration and the New Technological Borders of Europe*, edited by Huub Dijstelbloem and Albert Meijer, 1–21. Migration, Minorities and Citizenship. Palgrave Macmillan UK. http://link.springer.com/chapter/10.1057/9780230299382_1.
- Donaldson, Andrew, and David Wood. 2004. "Surveilling Strange Materialities: Categorisation in the Evolving Geographies of FMD Biosecurity." *Environment and Planning D: Society and Space* 22 (3): 373–91. doi:10.1068/d334t.
- Dredge, Stuart. 2013. "What Is Tor? A Beginner's Guide to the Privacy Tool." *The Guardian*, November 5, sec. Technology. <http://www.theguardian>.

- com/technology/2013/nov/05/tor-beginners-guide-nsa-browser.
- Dunn, Alix. 2016. "Responsible Data Leaks and Whistleblowing." The Engine Room. October 20. <https://www.theengineroom.org/responsible-data-leaks-and-whistleblowing/>.
- Electronic Frontier Foundation (EFF). 2013. "NSA Turns Cookies (And More) Into Surveillance Beacons." December 11. Accessed 13 February 2015. <https://www.eff.org/deeplinks/2013/12/nsa-turns-cookies-and-more-surveillance-beacons>.
- _____. 2014. "Timeline of NSA Domestic Spying." Accessed June 30. <https://www.eff.org/nl/nsa-spying/timeline>.
- _____. 2015. "Tor and HTTPS." Accessed February 11. <https://www.eff.org/pages/tor-and-https>.
- _____. "About EFF." n.d. Accessed August 2017. <https://www.eff.org/about>.
- Elmer, Greg. 2004. *Profiling Machines: Mapping the Personal Information Economy*. Cambridge, MA: MIT Press.
- Epstein, Steven. 1995. "The Construction of Lay Expertise: AIDS Activism and the Forging of Credibility in the Reform of Clinical Trials." *Science, Technology & Human Values* 20 (4): 408–37. doi:10.1177/016224399502000402.
- Evidon. 2013. "The Evidon Blog." Accessed March 7. <http://blog.evidon.com/tag/ghostery/>.
- _____. 2014a. "Analytics." Accessed January 25. <http://www.evidon.com/analytics>
- _____. 2014b. "Better Advertising Acquires Ghostery." Accessed January 30. <http://www.evidon.com/blog/better-advertising-acquires-ghostery>.
- "Facebook Resistance Workshop." 2011. By Tobias Leingruber (F.A.T.). Amsterdam, Mediamatic, April 22.
- Farman, Jason. 2014. "Creative Misuse as Resistance: Surveillance, Mobile Technologies, and Locative Games." *Surveillance & Society* 12 (3): 377–88. <http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/misuse>
- Fenster, Mark. 2012. "Disclosure's Effects: Wikileaks and Transparency" (July 28, 2011). Iowa Law Review, Vol. 97. Available at SSRN: <http://ssrn.com/abstract=1797945>
- Fernback, Jan. 2013. "Sousveillance: Communities of Resistance to the Surveillance Environment." *Telematics and Informatics*, The Facebook Phenomenon, 30 (1): 11–21. doi:10.1016/j.tele.2012.03.003.
- Forensic Architecture, ed. 2014. *Forensis: The Architecture of Public Truth*. London: Sternberg Press and Forensic Architecture. <http://www.sternberg-press.com/?pageId=1488>.
- Forensic Architecture. 2015. "Lexicon." Accessed October 22, 2015 Available at: <http://www.forensic-architecture.org/lexicon/forensis/>.
- Foucault, Michel. 1991 [1977]. *Discipline and Punish. The Birth of the Prison*. London etc.: Penguin Books.

- _____. 1998 [1976]. *The Will to Knowledge: The History of Sexuality: 1*. London: Penguin Books.
- Galison, Peter. 2016. "The Revelation of Secrets: Peter Galison and John May on Artifacts of Surveillance, Part I and II." *Thresholds* 43: 136-159; 254-267.
- Gallagher, Ryan, and Glenn Greenwald. 2014a. "How the NSA Plans to Infect 'Millions' of Computers with Malware." *The Intercept*. Accessed June 27. <https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/>.
- _____. 2014b. "Inside the NSA's Secret Efforts to Hunt and Hack System Administrators." *The Intercept*. Accessed June 27. <https://firstlook.org/theintercept/article/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/>.
- Garcia, David, and Geert Lovink. 1997. "The ABC of Tactical Media." *Nettime mailing list*, May 16. Accessed October 3, 2017. <http://www.nettime.org/Lists-Archives/nettime-l-9705/msg00096.html>.
- Garrido, Miguelángel Verde. 2015. "Contesting a Biopolitics of Information and Communications: The Importance of Truth and Sousveillance after Snowden." *Surveillance & Society* 13 (2): 153-67. http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/snowden_biopolitics.
- Gates, Kelly. 2013. "The Cultural Labor of Surveillance: Video Forensics, Computational Objectivity, and the Production of Visual Evidence." *Social Semiotics* 23 (2): 242-60. doi:10.1080/10350330.2013.777593.
- Gehl, Robert W. 2016. "Power/freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network." *New Media & Society* 18 (7): 1219-35. doi:10.1177/1461444814554900.
- Gerlitz, Carolin, and Anne Helmond. 2013. "The like Economy: Social Buttons and the Data-Intensive Web." *New Media & Society* 15 (8): 1348-65. doi:10.1177/1461444812472322.
- Ghostery 2014a. "Frequently Asked Questions." Accessed January 25. <https://www.ghostery.com/faq>.
- _____. "How It Works". Accessed January 20. <http://www.ghostery.com/how-it-works>.
- _____. 2014c. "What does Evidon do with Ghostrank information." Accessed April 3. <https://www.ghostery.com/faq#q17>.
- Ghostwords/chameleon. 2015. *Github*. Latest commit October 14. Accessed 2015, February 11. <https://github.com/ghostwords/chameleon#coverage>.
- Gitelman, Lisa, and Virginia Jackson. 2013. "Introduction." In *Raw Data Is an Oxymoron*, edited by Lisa Gitelman. Cambridge: MIT Press.
- Gonggrijp, Rop. 2014. "Surveillance: NOT a first world problem." Blog. *rop.gonggri.jp*. January 30. Accessed October 3, 2017. <https://rop.gonggri.jp/?p=722>.
- GOV.UK. 2016. "Policy Area: Government efficiency, transparency and accountability." Accessed August 9. <https://www.gov.uk/government/topics/government-efficiency-transparency-and-accountability>.

- Greenberg, Andy. 2012. *This Machine Kills Secrets: How WikiLeaks, Hacktivists and Cypherpunks Aim to Free the World's Information*. Virgin Books. <http://www.thismachinekillssecrets.com/>.
- Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. 1st edition. New York, NY: Metropolitan Books.
- Gregory, Sam. 2010. "Cameras Everywhere: Ubiquitous Video Documentation of Human Rights, New Forms of Video Advocacy, and Considerations of Safety, Security, Dignity and Consent." *Journal of Human Rights Practice* 00 (00): 11–17. doi:10.1093/jhuman/huq002.
- . 2012. "Human Rights Made Visible: New Dimensions to Anonymity, Consent, and Intentionality." In *Sensible Politics: The Visual Culture of Nongovernmental Activism*, edited by Meg McLagen and McKee, Yates, 551–63. New York: Zone Books.
- . 2015. "Yes, IBA still building it (based initially off InformaCam libraries)." March 25. 3:55 AM. <https://twitter.com/SamGregory/status/580684392319717376>.
- Grommé, Francisca. 2015. *Governance by Pilot Projects: Experimenting with Surveillance in Dutch Crime Control*. (Diss). Amsterdam: University of Amsterdam. <http://dare.uva.nl/record/1/486712>.
- Gurstein, Michael. 2010. "WikiLeaks, Open Information and Effective Use: Exploring the Limits of Open Government." *Gurstein's Community Informatics*. December 29. <https://gurstein.wordpress.com/2010/12/29/wikileaks-open-information-and-effective-use-exploring-the-limits-of-open-government/>.
- Hache, Alex. 2014. "Technological Sovereignty." In *For Free Information and Open Internet: Independent journalists, community media and hacktivists take action*, 166–171. Edited by Passerelle and Coredem. Ritimo, E-change platform.
- Hackett, Edward J., Olga Amsterdamska, Michael Lynch, and Judy Wajcman, eds. 2008. *The Handbook of Science and Technology Studies*. Third Edition. Cambridge, Massachusetts: The MIT Press. <https://mitpress.mit.edu/books/handbook-science-and-technology-studies>.
- Hagendijk, Rob. 1996. *Wetenschap, Constructivisme en Cultuur*. (Diss.) Universiteit van Amsterdam.
- Haggerty, Kevin. 2006. "Tear down the Walls: On Demolishing the Panopticon." In *Theorizing Surveillance: The Panopticon and Beyond*, edited by David Lyon. Devon: Willan Publishing.
- Haggerty, Kevin D., and Richard V. Ericson. 2000. "The Surveillance Assemblage." *The British Journal of Sociology* 51 (4): 605–22. doi:10.1080/00071310020015280.
- . 2006. "The New Politics of Surveillance and Visibility." In *The New Politics of Surveillance and Visibility*, edited by Kevin D. Haggerty and Richard V. Ericson. Toronto: University of Toronto Press..
- Haraway, Donna. 1988. "Situated Knowledges: The Science Question in

- Feminism and the Privilege of Partial Perspective." *Feminist Studies* 14 (3): 575–99. doi:10.2307/3178066.
- Harrison, Sarah. 2015. "Indexing the Empire". In *The WikiLeaks Files: The World According to US Empire*, edited by Wikileaks. London: Verso Books.
- Harvey, Penny, Madeleine Reeves, and Evelyn Ruppert. 2013. "Anticipating Failure." *Journal of Cultural Economy* 6 (3): 294–312. doi:10.1080/17530350.2012.739973.
- Heemsbergen, Luke J. 2013. "Radical Transparency in Journalism: Digital Evolutions from Historical Precedents." *Global Media Journal - Canadian Edition* 6 (1): 45–65.
- . 2014. "Designing Hues of Transparency and Democracy after WikiLeaks: Vigilance to Vigilantes and Back Again." *New Media & Society* 17 (8): 1340–57. doi:10.1177/1461444814524323.
- Helmond, Anne. 2012. "Trackers Gebruikt Op de Websites van Nederlandse Politieke Partijen in Kaart Gebracht." June 11. <http://www.annelhelmond.nl/2012/06/11/trackers-gebruikt-op-de-websites-van-nederlandse-politieke-partijen-in-kaart-gebracht/>.
- Hepp, Andreas. 2016. "Pioneer Communities: Collective Actors in Deep Mediatisation." *Media, Culture & Society* 38 (6): 918–33. doi:10.1177/0163443716664484.
- Hess, David J. 2005. "Technology- and Product-Oriented Movements: Approximating Social Movement Studies and Science and Technology Studies." *Science, Technology, & Human Values* 30 (4): 515–35.
- Hier, Sean Patrick, and Joshua Greenberg, eds. 2007. *The Surveillance Studies Reader*. Maidenhead etc.: Open University Press.
- . 2009. "David Murakami Wood's 'Situating Surveillance Studies.'" *Surveillance & Society* 7 (1): 71–75. <http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3309/3272>.
- Hindman, Elizabeth Blanks, and Ryan J. Thomas. 2014. "When Old and New Media Collide: The Case of WikiLeaks." *New Media & Society* 16 (4): 541–58. doi:10.1177/1461444813489504.
- Hine, Christine. 2007. "Multi-Sited Ethnography as a Middle Range Methodology for Contemporary STS." *Science, Technology & Human Values* 32 (6): 652–71. doi:10.1177/0162243907303598.
- Hintz, Arne. 2013. "Dimensions of Modern Freedom of Expression: WikiLeaks, Policy Hacking, and Digital Freedoms." In *Beyond WikiLeaks Implications for the Future of Communications, Journalism and Society*, edited by Benedetta Brevini, Arne Hintz, and Patrick McCurdy, 146–65. London: Palgrave Macmillan UK.
- Holmes, Harlo. 2011. "Inside the Augenblick: Digital Images, Metadata, and the Politics of Runtime." (MA thesis.) New York: NYU Steinhardt.
- Honan, Mat. 2012. "Oops! Did Vice Just Give Away John McAfee's Location With Photo Metadata?" *WIRED*. December 3. <http://www.wired.com/2012/12/oops-did-vice-just-give-away-john-mcafees-location-with->

this-photo/.

- Hoofnagle, Chris Jay, Ashkan Soltani, Nathan Good, Dietrich James Wambach, and Mika Ayenson. 2012. "Behavioral Advertising: The Offer You Cannot Refuse." *SSRN Scholarly Paper ID 2137601*. Rochester, NY: Social Science Research Network. <http://papers.ssrn.com/abstract=2137601>.
- Hutchinson, Sophie. 2013. "Social Media Plays Major Role in Turkey Protests." *BBC News*, June 4, 2013, sec. Europe. <http://www.bbc.com/news/world-europe-22772352>.
- "Identity Bureau Workshop." By Heath Bunting. Amsterdam, NIMk, 20 oktober 2011. <http://www.nimk.nl/nl/identity-bureau-workshop-hoe-maak-je-een-nieuwe-identiteit>.
- "Interference Conference." 2014. Interference: Three days of critical approaches to technology, Amsterdam, August 15-17. <https://web.archive.org/web/20141013174221/http://interference.io:80/>
- International Bar Association. 2015. "About the IBA." Accessed February 18. <http://www.ibanet.org/>.
- Internet Protection Lab. 2014. "FinFisher hack: The Bahrain Logs." August 11. <https://internetprotectionlab.net/2014/08/09/finfisher-hack-the-bahrain-logs/>.
- Jasanoff, Sheila. 1998a. "Judging Science: Issues, Assumptions, Models." Scientific Evidence In *The Courts: Concepts & Controversies: Report of the 1997 Forum for State Court Judges*, The Roscoe Pound Foundation.
- . 1998b. "The Eye of Everyman Witnessing DNA in the Simpson Trial." *Social Studies of Science* 28 (5-6): 713-40. doi:10.1177/030631298028005003.
- JSON Evidentiary Mobile Media Metadata. 2013. Accessed June 6. <http://j3m.info>.
- Jurgenson, Nathan, and P. J. Rey. 2014. "Liquid Information Leaks." *International Journal of Communication* 8 (0): 14. <http://ijoc.org/index.php/ijoc/article/view/2947>.
- Keenan, Thomas. 2014. "Counter-Forensics and Photography." *Grey Room* (55): 58-77. doi:10.1162/GREY_a_00141.
- Kelty, Christopher. 2008. "Geeks and Recursive Publics." In *Two Bits: The Cultural Significance of Free Software*. Duke University Press.
- King, Nancy J., and Pernille Wegener Jessen. 2010. "Profiling the Mobile Customer - Is Industry Self-Regulation Adequate to Protect Consumer Privacy When Behavioural Advertisers Target Mobile Phones? - Part II." *Computer Law & Security Review* 26 (6): 595-612. doi:16/j.clsr.2010.09.007.
- Knorr-Cetina, Karin, and Werner Reichmann. 2015. "Epistemic Cultures A2 - Wright, James D." In *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)*, 873-80. Oxford: Elsevier. <http://www.sciencedirect.com/science/article/pii/B9780080970868104544>.
- Koop, Peter. 2014. "Top Level Telecommunications: Snowden-Documents Show No Evidence for Global Mass Surveillance." Accessed June 30.

- <http://electrospace.blogspot.nl/2014/06/snowden-documents-show-no-evidence-for.html>.
- Koot, Matthijs. 2012. "A Survey of Privacy & Security Decreasing Third-Party Content on Dutch Websites," October 26. <http://www.madison-gurkha.com/press/2012-10-SurveyOfThirdPartyContent.pdf>.
- Landau, Susan. 2013. "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations." *IEEE Security & Privacy* 11 (4): 54–63.
- Langlois, Ganaele, Greg Elmer, Fenwick McKelvey, Zachary Devereaux. 2009. "Networked Publics: The Double Articulation of Code and Politics on Facebook." *Canadian Journal of Communication* 34 (3): 415-434. doi: 10.22230/cjc.2009v34n3a2114.
- Larson, Jeff, James Glanz, Andrew W. Lehren. 2014. "Spy Agencies Probe Angry Birds and Other Apps for Personal Data." *ProPublica (in collaboration with the New York Times)*. January 27. Accessed June 27, 2014: <http://www.propublica.org/article/spy-agencies-probe-angry-birds-and-other-apps-for-personal-data>.
- Latour, Bruno. 1983. "Give Me a Laboratory and I Will Raise the World." In *Science Observed: Perspectives on the Social Study of Science*, edited by Karin D Knorr-Cetina and Michael Mulkay. London: Sage Publications.
- . 1986. "Visualisation and Cognition: Drawing Things Together." *Knowledge and Society Studies in the Sociology of Culture Past and Present*, edited by Henrika Kuklick. *Jai Press* 6: 1–40.
- . 1987. *Science in Action: How to Follow Scientists and Engineers through Society*. Harvard University Press.
- . 1993. *The Pasteurization of France*. Harvard University Press.
- . 2004. *Politics of Nature: How to Bring the Sciences into Democracy*. Cambridge, Mass, etc: Harvard University Press.
- . 2005a. "From Realpolitik to Dingpolitik: or How to Make Things Public." In *Making Things Public: Atmospheres of Democracy*, edited by Bruno Latour and Peter Weibel, 14-42. ZKM Center for Media Karlsruhe. Cambridge, Massachusetts: MIT Press. <http://www.bruno-latour.fr/node/208>.
- . 2005b. *Reassembling the Social : An Introduction to Actor-Network-Theory*. Oxford ;New York: Oxford University Press.
- . 2010. *The Making of Law: An Ethnography of the Conseil d'Etat*. Cambridge, UK; Malden, MA: Polity.
- . 2012. "The Production of Public Proof, Centre for Research Architecture." Transcript of lecture. March 5. Accessed December 12, 2014. <http://www.forensic-architecture.org/seminar/production-public-proof/>.
- Latour, Bruno, and Peter Weibel. 2005. *Making Things Public: Atmospheres of Democracy*. 1st edition. Cambridge, MA; Karlsruhe, Germany: MIT Press.
- Law, John. 1992. "Notes on the Theory of the Actor-Network: Ordering, Strategy, and Heterogeneity." *Systems Practice* 5 (4): 379–93. doi:10.1007/BF01059830.

- . 1997. “Traduction/Trahison – Notes on ANT.” published by the Department of Sociology Lancaster University. <http://cseweb.ucsd.edu/~goguen/courses/175/stslaw.html>.
- Law, John, and John Urry. 2004. “Enacting the Social.” *Economy and Society* 33 (3): 390–410. doi:10.1080/0308514042000225716.
- Legal Information Institute (LII). 2013. “Daubert Standard.” Accessed August 13. http://www.law.cornell.edu/wex/daubert_standard.
- Leistert, Oliver. 2013. “Smell the Fish: Digital Disneyland and the Right to Oblivion.” *First Monday* 18 (3). <http://www.firstmonday.org/ojs/index.php/fm/article/view/4619>.
- Leonardi, Paul M. 2010. “Digital Materiality? How Artifacts without Matter, Matter.” *First Monday* 15 (6). <http://firstmonday.org/ojs/index.php/fm/article/view/3036>.
- Lievrouw, Leah A. 2014. “WikiLeaks and the Shifting Terrain of Knowledge Authority.” *International Journal of Communication* 8 (0): 15. <http://ijoc.org/index.php/ijoc/article/view/2667>.
- Lovink, Geert, and Miriam Rasch, eds. 2013. *Unlike Us Reader: Social Media Monopolies and Their Alternatives*. Amsterdam: Institute of Network Cultures.
- Lovink, Geert, and Ned Rossiter. 2011. “Seriality for All the Role of Protocols and Standards in Critical Theory.” In *Interoperabel Nederland*, edited by Pieter Wisse, 427–33. Den Haag: Forum Standaardisatie.
- . 2012. “In Praise of Concept Production.” In *The International Encyclopedia of Media Studies*, edited by Angharad N. Valdivia. Blackwell Publishing Ltd. <http://onlinelibrary.wiley.com/doi/10.1002/9781444361506.wbiems142/abstract>.
- Lovink, Geert, and Patrice Riemens. 2013. “Twelve Theses on WikiLeaks.” In *Beyond WikiLeaks Implications for the Future of Communications, Journalism and Society*, edited by Benedetta Brevini, Arne Hintz, and Patrick McCurdy, 245–53. London: Palgrave Macmillan UK.
- Lury, Celia, and Nina Wakeford. 2014 [2012]. *Inventive Methods: The Happening of the Social*. Abingdon: Routledge. <http://www.routledge.com/books/details/9780415574815/>.
- Lynch, Michael. 1998. “The Discursive Production of Uncertainty The OJ Simpson ‘Dream Team’ and the Sociology of Knowledge Machine.” *Social Studies of Science* 28 (5–6): 829–68. doi:10.1177/030631298028005007.
- Lyon, David. 1994. “Challenging Surveillance.” In *The Electronic Eye: The Rise of Surveillance Society*, edited by David Lyon. Ambridge: Polity Press.
- . 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.
- . 2003. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge.
- . 2006. *Theorizing Surveillance: The Panopticon and beyond*. Devon: Willan Publishing.

- . 2007. *Surveillance Studies: An Overview*. Cambridge: Polity.
- . 2013. "Introduction." In *Liquid Surveillance: A Conversation*. Edited by Zygmunt Bauman, David Lyon, 1-17. Cambridge: Polity Press.
- "Making Cameras Count." 2013. *Google Ideas - Conflict in a Connected World*, October 24. Accessed January 20, 2015. https://www.youtube.com/watch?feature=player_embedded&v=lzjoAdhAKWU.
- Mann, Steve. 2004. "'Sousveillance' Inverse Surveillance in Multimedia Imaging." Conference: Proceedings of the 12th ACM International Conference on Multimedia, New York, NY, USA, October 10-16, 2004 620-27. doi:10.1145/1027527.1027673.
- Mann, Steve, and Joseph Ferenbok. 2013. "New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World." *Surveillance & Society* 11 (1/2): 18-34. <http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/veillance>.
- Mann, Steve, Jason Nolan, and Barry Wellman. 2003. "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments." *Surveillance & Society* 1 (3): 331-355. <http://www.surveillance-and-society.org/articles1%283%29/sousveillance.pdf>.
- Manovich, Lev. 2001. *The Language of New Media*. MIT Press. http://newmedia.wikia.com/wiki/The_Language_of_New_Media.
- Marres, Noortje. 2005. *No Issue, No Public: Democratic Deficits after the Displacement of Politics*. (Diss.) Universiteit van Amsterdam. <http://dare.uva.nl/record/165542>.
- . 2011. "The Costs of Public Involvement: Everyday Devices of Carbon Accounting and the Materialization of Participation." *Economy and Society* 40 (4): 510-33. doi:10.1080/03085147.2011.602294.
- . 2012a. *Material Participation: Technology, the Environment and Everyday Publics*. London: Palgrave Macmillan.
- . 2012b. "The Redistribution of Methods: On Intervention in Digital Social Research, Broadly Conceived." *The Sociological Review* 60: 139-165. doi:10.1111/j.1467-954X.2012.02121.x.
- Marres, Noortje, and Javier Lezaun. 2011. "Materials and Devices of the Public: An Introduction." *Economy and Society* 40 (4): 489-509. doi:10.1080/03085147.2011.602293.
- Marres, Noortje, and Richard Rogers. 2008. "Subsuming the ground: how local realities of the Ferghana valley, the Narmada dams and the BTC pipeline are put to use on the web." *Economy and Society*, 37 (2): 251-281. doi: 10.1080/03085140801933314.
- Marres, Noortje, and Esther Weltevrede. 2013. "Scraping the Social?" *Journal of Cultural Economy*, February, 1-23. doi:10.1080/17530350.2013.772070.
- Martijn, Maurits. 2014. "Hoe Doe Je Dat: Privacy Verkopen?" *De Correspondent*. February 21. <https://decorrespondent.nl/756/Hoe-doe-je-dat-privacy-verkopen-/23251536-076e2f59>.
- Martin, Aaron K, Rosamunde E van Brakel, and Daniel J Bernhard. 2009.

- “Understanding Resistance to Digital Surveillance: Towards a Multi-Disciplinary, Multi-Actor Framework.” *Surveillance & Society* 6 (3): 213–32. <http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3282>
- Marx, Gary T. 2002. “What’s New About the ‘New Surveillance’? Classifying for Change and Continuity.” *Surveillance & Society* 1 (1): 9–29. <http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3391>
- _____. 2012. “‘Your Papers Please’: Personal and Professional Encounters With Surveillance.” In *International Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin Haggerty, and David Lyon. Oxon; New York: Routledge.
- Mattern, Shannon. 2013. “Infrastructural Tourism.” *Places Journal*, July. doi:<https://doi.org/10.22269/130701>.
- Maxigas. 2014a. “Hacklabs and Hackerspaces – Tracing Two Genealogies.” *The Journal of Peer Production* 2. <http://peerproduction.net/issues/issue-2/peer-reviewed-papers/hacklabs-and-hackerspaces/>.
- _____. 2014b. “Hacklabs and Hackerspaces: Shared Machine Workshops.” In *For Free Information and Open Internet: Independent journalists, community media and hacktivists take action*, 146–154. Edited by Passerelle and Coredem. Ritimo, E-change platform.
- McDonald, Aleecia M. and Lorrie Faith Cranor. 2008. “The cost of reading privacy policies.” *I/S: A Journal of Law and Policy for the Information Society* 4 (3): 540–565.
- M’charek, Amade. 2008. “Silent Witness, Articulate Collective: DNA Evidence and the Inference of Visible Traits.” *Bioethics* 22 (9): 519–28. doi:10.1111/j.1467-8519.2008.00699.x.
- McStay, Andrew. 2013. “I Consent: An Analysis of the Cookie Directive and Its Implications for UK Behavioral Advertising.” *New Media & Society* 15 (4): 596–611. doi:10.1177/1461444812458434.
- McQuillan, Dan. 2013. “From Free Software to Artisan Science.” *Journal of Peer Production* 3. <http://peerproduction.net/issues/issue-3-free-software-epistemics/peer-reviewed-papers/from-free-software-to-artisan-science/>.
- _____. 2014. “Research Reflections: Collaborative Research and the Hacker Ethic.” *Creativeworks London News Archive*. August. <http://www.creativeworkslondon.org.uk/cw-news/research-reflections-collaborative-research-and-the-hacker-ethic/>
- Milan, Stefania. 2010. “SSRC| Introduction: Toward An Epistemology of Engaged Research | Making Communication Research Matter.” *International Journal of Communication* 4 (0):3. <http://ijoc.org/index.php/ijoc/article/view/915/460>.
- _____. 2013. *Social Movements and Their Technologies: Wiring Social Change*. Palgrave Macmillan UK: London.
- Modderkolk, Huib. 2016. “De dreiging is in jaren niet zo groot geweest.” *De Volkskrant*, September 17. Accessed December 8, 2016: <http://www.volkskrant.nl/binnenland/-dreiging-is-in-jaren-nog-niet-zo-groot->

- geweest~a4378383/.
- Mol, Annemarie. 2002. *The Body Multiple: Ontology in Medical Practice*. Durham, NC, etc: Duke University Press.
- . 2010. "Actor-Network Theory: sensitive terms and enduring tensions." *Kölner Zeitschrift für Soziologie und Sozialpsychologie*. Sonderheft, 50, 253-269.
- Mommers, Jelmer, and Maurits Martijn. 2016. "Waarom de Opwarming van de Aarde Een Geschenk Is Voor Privacystrijders." *De Correspondent*. October 6, 2016. <https://decorrespondent.nl/5376/waarom-de-opwarming-van-de-aarde-een-geschenk-is-voor-privacystrijders/592483584-44304951>.
- Monahan, Torin. 2006. "Counter-Surveillance as Political Intervention?" *Social Semiotics* 16 (4): 515–34. doi:10.1080/10350330601019769.
- Morozov, Evgeny. 2009 "How Dictators Watch Us on the Web." *Prospect Magazine*. November 9. Accessed October 23, 2017. <https://www.prospectmagazine.co.uk/magazine/how-dictators-watch-us-on-the-web>.
- Mortensen, Mette. 2014. "Who Is Surveilling Whom? Negotiations of Surveillance and Sousveillance in Relation to WikiLeaks' Release of the Gun Camera Tape Collateral Murder." *Photographies* 7 (1): 23–37. doi:10.1080/17540763.2014.896144.
- Murakami Wood, David. 2007. "Beyond the Panopticon? Foucault and Surveillance Studies." In *Space, Knowledge and Power: Foucault and Geography*, edited by Jeremy W. Crampton and Stuart Elden. Hampshire: Ashgate.
- . 2009. "Situating Surveillance Studies. Sean Hier and Josh Greenberg's The Surveillance Studies Reader, and David Lyon's Surveillance Studies: An Overview." *Surveillance & Society* 6 (1): 52–61.
- Murakami Wood, David, and Steve Wright. 2015. "Before and After Snowden." *Surveillance & Society* 13 (2): 132–38. <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/5710>
- "Occupy Technology". 2012. Schijnheilig@Vondelbunker, Amsterdam. 11 March. Accessed October 3, 2017. <https://schijnheilig.nul.nu/2012/03/occupy-technology/>
- O'Neill, Kathleen, Della Sentilles and Daniel M. Brinks. 2011. "New Wine in Old Wineskins? New Problems in the Use of Electronic Evidence in Human Rights Investigations and Prosecutions." Bernard and Audre Rapoport Center for Human Rights and Justice. University of Texas at Austin School of Law.
- Open Whisper Systems. 2014. "Open Whisper Systems partners with WhatsApp to provide end-to-end encryption." November 18. Accessed February 11, 2015. <https://whispersystems.org/blog/whatsapp/>.
- "Operation Pursuant." 2012. *Pastebin*. September 6. <http://pastebin.com/iHFxBiHv>
- Parikka, Jussi. 2007. *Digital Contagions: A Media Archaeology of Computer Viruses*. Digital Formations Vol. 44. New York, NY etc: Peter Lang.
- PEN American Center. 2014. "PEN Surveillance Metaphor Mapping Project."

- April 8. Accessed June 27, 2014: <http://www.pen.org/infographic/pen-surveillance-metaphor-mapping-project>.
- Poitras, Laura. *Citizen Four*. 2014.
- Poitras, Laura, Marcel Rosenbach, Fidelius Schmid, Holger Stark, and Jonathan Stock. 2013. "Cover Story: How the NSA Targets Germany and Europe." *Spiegel Online*, January 7. Accessed June 30, 2014: <http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html>.
- Poster, Mark. 2008. "Foucault, Deleuze, and New Media", 'Foucault Across the Disciplines' Conference, UCSC, March 1. Accessed August 27, 2015: <http://humweb.ucsc.edu/foucaultacrossthedisciplines/foucault.htm>.
- Prainsack, Barbara, and Victor Toom. 2010. "The Prüm Regime: Situated Dis/Empowerment in Transnational DNA Profile Exchange." *British Journal of Criminology* 50 (6): 1117–35. doi:10.1093/bjc/azq055.
- Pridmore, Jason. n.d. "Consumer Surveillance: Context, Perspectives and Concerns in the Personal Information Economy." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin D. Haggerty, and David Lyon, 321–30. London: Routledge.
- Quill, Lawrence. 2014. *Secrets and Democracy: From Arcana Imperii to WikiLeaks*. Basingstoke, GB: Palgrave Macmillan.
- Raghavan, Sriram. 2013. "Digital Forensic Research: Current State of the Art." *CSI Transactions on ICT* 1 (1): 91–114. doi:10.1007/s40012-012-0008-7.
- Raley, Rita. 2013. "Dataveillance and Countervailence." In *"Raw Data" is an Oxymoron*, edited by Lisa Gitelman. Cambridge, Massachusetts: MIT Press.
- Rathenau Instituut. 2007. "Van Privacyparadijs Tot Controlestaat? Misdaad-En Terreurbestrijding in Nederland Aan Het Begin van de 21ste Eeuw." Studie 49. Den Haag: Rathenau Instituut.
- Reigeluth, Tyler Butler. 2014. "Why Data Is Not Enough: Digital Traces as Control of Self and Self-Control." *Surveillance & Society* 12 (2): 243–54. <http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/enough>
- Reilly, Paul. 2015. "Every Little Helps? YouTube, Sousveillance and the 'anti-Tesco' Riot in Stokes Croft." *New Media & Society* 17 (5): 755–71. doi:10.1177/1461444813512195.
- Rogers, Richard. 2004. *Information Politics on the Web*. Cambridge, Massachusetts. MIT Press.
- _____. 2005. "New Media Effects: Do Formats Organize Networks?" *Complexity* 10 (5). doi: 10.1002/cplx.20083.
- _____. 2008. "Consumer Technology after Surveillance Theory." In *Mind the Screen: Media Concepts according to Thomas Elsaesser*, edited by Jaap Kooijman, Patricia Pisters, and Wanda Strauven, 288–296.
- _____. 2009a. "Post-Demographic Machines." In *Walled Garden*, edited by Annet Dekker and Anette Wolfsberger, 29–39. Amsterdam: Virtueel Platform.

- . *The end of the virtual: Digital methods*. Amsterdam: Amsterdam University Press, 2009b: 1-38.
- . 2013. *Digital Methods*. Cambridge, Massachusetts: MIT Press.
- Rogers, Richard, Esther Weltevrede, Sabine Niederer, and Erik Borra. n.d. "National Web Studies: The Case of Iran Online." In *A Companion to New Media Dynamics*, edited by J. Hartley, A. Bruns, and J. Burgess, 142–66. Oxford: Blackwell.
- Rosen, David, and Aaron Santesso. 2013. "The Eye of Sauron Is the Modern Surveillance State." *Slate*, July 17. http://www.slate.com/articles/news_and_politics/jurisprudence/2013/07/tolkien_v_orwell_who_understood_modern_surveillance_best.html.
- Ruppert, Evelyn. 2015. "Doing the Transparent State: Open Government Data as Performance Indicators." In *A World of Indicators: The Making of Governmental Knowledge through Quantification*, edited by R. Rottenburg, S. E. Merry, S.-J. Park, and J. Mugler, 1–18. Cambridge: Cambridge University Press. <http://eprints.gold.ac.uk/8302/>.
- Ruppert, Evelyn, John Law, and Mike Savage. 2013. "Reassembling Social Science Methods: The Challenge of Digital Devices." *Theory, Culture & Society* 30 (4): 22–46. doi:10.1177/0263276413484941.
- Savage, Mike, and Roger Burrows. 2007. "The Coming Crisis of Empirical." *Sociology* 41 (5): 885–99. doi:10.1177/0038038507080443.
- Savage, Mike, Evelyn Ruppert, and John Law. 2010. "Digital Devices: nine theses." *CRESC Working Paper Series*, Working Paper No. 86. <http://www.cresc.ac.uk/medialibrary/workingpapers/wp86.pdf>
- Schneier, Bruce. 2013. "Attacking Tor: How the NSA Targets Users' Online Anonymity." *The Guardian*, October 4, sec. World news. <http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity>.
- Schoemaker, René. 2012. "Cookiewet Genegeerd Door Grote Nederlandse Sites." *Webwereld*. August 3. Accessed October 27, 2017. <http://webwereld.nl/e-commerce/57590-cookiewet-genegeerd-door-grote-nederlandse-sites>.
- Schuilenberg, Marc. 2009. "Assemblages." In *Deleuze Compendium*, edited by E. Romein, M. Schuilenberg, and S. van Tuinen, 205-223. Amsterdam: Boom,
- Schuppli, Susan. 2013. "Material Witness." *Art Critical Lecture Series*. Goldsmiths College, March 11. Accessed December 12, 2014. <http://magiclantern.gold.ac.uk/podcasts/art/SusanSchuppli.mp3>.
- . 2014. "Entering Evidence: Cross-Examining the Court Records of the Icty." In *Forensis: The Architecture of Public Truth*, edited by Forensic Architecture, 279-316. Berlin: Sternberg Press.
- . (forthcoming.) *Material Witness*, edited by D. Sery. London: MIT Press.
- Sedona. 2007. *The Sedona Principles (Second Edition): Best Practices Recommendations & Principles for Addressing Electronic Document Production*. The Sedona Conference. Accessed August 31, 2013. http://www.sos.mt.gov/Records/committees/erim_resources/A%20-%20Sedona%20

- Principles%20Second%20Edition.pdf.
- Shapin, Steven, and Simon Schaffer. 1985. *Leviathan and the Air-Pump: Hobbes, Boyle, and the Experimental Life*. Princeton, N. J.: Princeton University Press.
- Signals: Exhibition of the Snowden Files in Art, Media and Archives. Curated by Magdalena Taube and Krystian Woznicki, Berlin. September 12 – November 1, 2017. <http://berlingazette.de/signals/>.
- Silverman, Craig. 2014. "Verification Tools." In *Verification Handbook: A Definitive Guide to Verifying Digital Content for Emergency Coverage*. European Journalism Centre (EJC). <http://verificationhandbook.com/book/chapter10.php>.
- Simon, Bart. 2005. "The Return of Panopticism: Supervision, Subjection and the New Surveillance." *Surveillance & Society* 3 (1): 1–20.
- Sismondo, Sergio. 2003. *An Introduction to Science and Technology Studies*. Malden, MA: Wiley-Blackwell.
- Snickars, Pelle. 2014. "Himalaya of Data." *International Journal of Communication* 8 (0): 13. <http://ijoc.org/index.php/ijoc/article/view/2892>
- "Snowden Surveillance Archive." n.d. Accessed October 27, 2017. <https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi>.
- "Snowden Files For All?" 2014. *An initiative by Berliner Gazette*. http://berlingazette.de/wp-content/uploads/BG_UNCOMMONS_SFA-Initiative-2015_EN.pdf.
- Soltani, Ashkan, Andrea Peterson, and Barton Gellman. 2013a. "New Documents Show How the NSA Infers Relationships Based on Mobile Location Data." *The Washington Post*, December 10. <https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/>.
- _____. 2013b. "NSA Uses Google Cookies to Pinpoint Targets for Hacking." *The Washington Post*, December 10. <https://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking>.
- SPIEGEL Staff. 2013a. "GHCQ Targets Engineers with Fake LinkedIn Pages." *Spiegel Online*, November 11. <http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html>.
- _____. 2013b. "Inside TAO: Targeting Mexico." *Spiegel Online*, December 29. <http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-2.html>.
- Stalder, Felix. 2002. "Privacy Is Not the Antidote to Surveillance." *Surveillance & Society* 1 (1): 120–24. <http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3397>.
- Star, Susan Leigh, and James R. Griesemer. 1989. "Institutional Ecology, 'Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907–39." *Social Studies of Science* 19 (3): 387–420. <http://www.jstor.org.proxy.uba.uva.nl/2048/stable/285080>.

- “Surveillance Studies Forschernetzwerk.” 2016. Accessed August 14. (<http://www.surveillance-studies.org/forschernetzwerk/>).
- Sutko, Daniel M., and Adriana de Souza e Silva. 2011. “Location-Aware Mobile Media and Urban Sociability.” *New Media & Society*, March, 1461444810385202. doi:10.1177/1461444810385202.
- Tanczer, Leonie. 2015. “Hacking the Label: Hacktivism, Race, and Gender.” *Ada: A Journal of Gender, New Media, and Technology* 6 (January). <http://adanewmedia.org/2015/01/issue6-tanczer/>.
- Telecommunicatiewet. 2012. “Artikel 11.7a”. Accessed August 14, 2016. http://wetten.overheid.nl/BWBR0009950/Hoofdstuk11/i111/Artikel117a/geldigheidsdatum_03-09-2012.
- The Citizen Lab. 2012. “From Bahrain With Love: FinFisher’s Spy Kit Exposed.” Accessed August 27, 2015. <https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/>.
- The Critical Engineering Working Group. 2011-2017. “The Critical Engineering Manifesto.” Berlin, October. Accessed October 3, 2017. <https://www.criticalengineering.org/>.
- The Guardian. 2013a. “Tor Stinks’ Presentation – Read the Full Document.” *The Guardian*, October 4, sec. World news. Accessed June 30, 2014: <http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document>.
- The Guardian. 2013b. “Tor: ‘The King of High-Secure, Low-Latency Anonymity.’” *The Guardian*, October 4, sec. World news. Accessed June 30, 2014: <http://www.theguardian.com/world/interactive/2013/oct/04/tor-high-secure-internet-anonymity>.
- The Guardian Project. 2012. “Introducing InformaCam.” Accessed August 31, 2013. <http://guardianproject.info/2012/01/20/introducing-informacam/>.
- . 2013a. “About The Guardian Project.” Accessed August 31, 2013. <http://guardianproject.info>.
- . 2013b. “ObscuraCam: Secure Smart Camera.” Accessed August 31, 2013. <http://guardianproject.info/apps/obscuracam/>.
- . n.d. “SecureSmartCam » CameraV (InformaCam Project).”. n.d. Accessed March 2013. <https://dev.guardianproject.info/projects/informacam>.
- The Human Rights Center at the University of California. 2012. “Beyond Reasonable Doubt: Using Scientific Evidence to Advance Prosecutions at the International Criminal Court.” Workshop Report 23-24. University of California, Berkeley, School of Law.
- The Intercept. 2014. “How the NSA Secretly Masqueraded as Facebook to Hack Computers for Surveillance.” March 11. <https://vimeo.com/88822483>
- “The Rashomon Project: an Open-Source Toolkit for Assembling and Analyzing Multi-Perspective Video Timelines.” 2015. A project by UC Berkeley CITRIS Data and Democracy Initiative with Witness.org, The Guardian Project, The Berkeley Human Rights Center, and The UC Santa

- Cruz Digital Arts and New Media Program. Accessed 20 January, 2015. <http://automation.berkeley.edu/rashomon/>.
- The Third Party Diary: Een onderzoek naar derde partijen op overheidswebsite. 2012. <http://thirdpartydiary.net>.
- Timan, Tjerk. 2013. *Changing landscapes of Surveillance: Emerging Technologies and Participatory Surveillance in Dutch Nightscapes*. (Diss.) Enschede, 6 November. <http://doc.utwente.nl/87623/>.
- Timan, Tjerk, and Nelly Oudshoorn. 2012. "Mobile Cameras as New Technologies of Surveillance? How Citizens Experience the Use of Mobile Cameras in Public Nightscapes." *Surveillance & Society* 10 (2): 167–81. <http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/mobiles>
- Toom, Victor. 2010. "Inquisitorial Forensic DNA Profiling in the Netherlands and the Expansion of the Forensic Genetic Body." In *Genetic Suspects. Global Governance of Forensic DNA Profiling and Databasing*, edited by R. Hindmarsh and Barbara Prainsack, 175–95. Cambridge: Cambridge University Press.
- Tor. 2015. "Tor: Overview." Accessed January 20. <https://www.torproject.org/about/overview.html.en>.
- "Track the Trackers." 2012. *Digital Methods Winter School: Interfaces for the Cloud*. Project members: Yngvil Beyer, Erik Borra, Carolin Gerlitz, Anne Helmond, Koen Martens, Simeona Petkova, JC Plantin, Bernhard Rieder, Lonke van der Velden, Esther Weltevrede. <https://wiki.digitalmethods.net/Dmi/DmiWinterSchool2012TrackingTheTrackers>.
- Tran, Minh, Xinshu Dong, Zhenkai Liang, and Xuxian Jiang. 2012. "Tracking the Trackers: Fast and Scalable Dynamic Analysis of Web Content for Privacy Violations." In *Applied Cryptography and Network Security*, 418–435. Springer. http://link.springer.com/chapter/10.1007/978-3-642-31284-7_25.
- Transnational Institute (TNI). 2017. "Culture of the Commons: Interview with Mayo Fuster Morell." *TNI*. January 27. <https://www.tni.org/en/transnational-institute>.
- Tuters, Marc, and Kazys Varnelis. 2006. "Beyond Locative Media: Giving Shape to the Internet of Things." *Leonardo* 39 (4): 357–63. <https://muse.jhu.edu/article/200367/pdf>
- Van Buuren, Jelle. 2014. "From Oversight to Undersight: The Internationalization of Intelligence." *Security and Human Rights* 24 (3-4): 239–52. doi:10.1163/18750230-02404003.
- Van den Berg, Bibi, and Simone van der Hof. 2012. "What Happens to My Data? A Novel Approach to Informing Users of Data Processing Practices." *First Monday* 17 (7). doi:10.5210/fm.v17i7.4010.
- Van der Ploeg, Irma. 1999. "The Illegal Body: 'Eurodac' and the Politics of Biometric Identification." *Ethics and Information Technology* 1 (4): 295–302. doi:10.1023/A:1010064613240.
- Van der Velden, Lonke. 2014. "The Third Party Diary: Tracking the trackers

- on Dutch governmental websites. *NECSUS. European Journal of Media Studies* 3 (1): 195-217. doi: <http://dx.doi.org/10.5117/NECSUS2014.1>.
- . 2015. "Forensic devices for activism: Metadata tracking and public proof." *Big Data & Society* 2 (2). doi: 10.1177/2053951715612823.
- . 2015. "Leaky Apps and Data Shots: Leakage and Insertion in NSA-surveillance." *Surveillance & Society* 13 (2): 182-196. http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/snowden_leakage.
- Van Koppen, Peter J. 2007. "Miscarriages of Justice in Inquisitorial and Accusatorial Legal Systems." *Journal of the Institute of Justice and International Studies* 7: 50. <http://heinonline.org/HOL/Page?handle=hein.journals/jijis7&id=58&div=&collection=journals>.
- Van 't Hof, Christian, and Rinie van Est. 2010. *Check in - Check uit: de digitalisering van de openbare ruimte*. Edited by Christian van 't Hof, Rinie van Est, and Floortje Daemen. Rotterdam: Nai Uitgevers/Publishers.
- Vennesson, Pascal. 2008. "Case Studies and Process Tracing: Theories and Practices." In *Approaches and Methodologies in the Social Sciences: A Pluralist Perspective*, edited by Donatella della Porta and Michael Keating, 223-39. Cambridge: Cambridge University Press.
- VPRO. 2014. "Charlie Stross". February 25. *VPRO Tegenlicht*. <https://www.vpro.nl/programmas/tegenlicht/lees/biografieen/s/charles-stross.html>.
- Watson, Trevor. 2015. "Admissible Evidence?" *Saakshi Project*. n.d. Accessed October 27 2017. <http://www.saakshiproject.com/lawyers/admissible-evidence.html>.
- "Websiteregister Rijksoverheid." 2013. Accessed January 25. <http://www.rijksoverheid.nl/onderwerpen/overheidscommunicatie/eisen-aan-websites-rijksoverheid/websiteregister-rijksoverheid>.
- Weizman Eyal. 2013. "Forensis: the architecture of public truth." Inaugural lecture. Goldsmiths College, University of London, 24 October.
- . 2014. "Introduction: Forensis." In *Forensis: The Architecture of Public Truth*, edited by Forensic Architecture, 9-32. London: Sternberg Press and Forensic Architecture.
- Weizman, Eyal, Paulo Tavares, Susan Schuppli, and Situ Studio. 2010. "Forensic Architecture." *Architectural Design* 80 (5): 58-63. doi:10.1002/ad.1134.
- Weltevrede, Esther. 2016. *Repurposing Digital Methods: The Research Affordances of Platforms and Engines*. (Diss.). University of Amsterdam. <http://hdl.handle.net/11245/1.505660>.
- Westlake, E. J. 2008. "Friend Me If You Facebook: Generation Y and Performative Surveillance." *TDR: The Drama Review* 52 (4): 21-40.
- WikiLeaks. 2012. "The Global Intelligence Files." February 27. <https://wikileaks.org/the-gifiles.html>.
- . 2013. "The Spyfiles 3." September 3. Accessed 2016, August 9. <https://wikileaks.org/spyfiles3p.html>.

- . 2015. *The WikiLeaks Files: The World According to US Empire*. London: Verso Books.
- . 2016. "What is WikiLeaks." Accessed August 9. <https://wikileaks.org/What-is-Wikileaks.html>.
- WikiLeaks Press. 2016. Accessed 19 March. <http://www.wikileaks-press.org>.
- Wikipedia. 2015. "Leakage." Wikipedia, the Free Encyclopedia. Accessed February 11. <https://en.wikipedia.org/wiki/Leakage>.
- Wikipedia. 2016. "Edward Snowden." Wikipedia, the Free Encyclopedia. Accessed July 21. https://en.wikipedia.org/wiki/Edward_Snowden.
- Winner, Langdon. 1980. "Do Artifacts Have Politics?" *Daedalus* 109 (1): 121–36. <http://www.jstor.org.proxy.uba.uva.nl:2048/stable/20024652>
- Winseck, Dwayne. 2013. "Weak Links and WikiLeaks: How Control of Critical Internet Resources and Social Media Companies' Business Models Undermine the Networked Free Press." In *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*, edited by Benedetta Brevini, Arne Hintz, and Patrick McCurdy, 166–77. London: Palgrave Macmillan UK.
- Witness. 2011. *Cameras Everywhere Report 2011*. Accessed August 31, 2013. <http://www.witness.org/cameras-everywhere/report-2011/table-of-contents>.
- . 2012. "Visual Anonymity and YouTube's New Blurring Tool." *WITNESS Blog*. Accessed January 20, 2015. <http://blog.witness.org/2012/07/visual-anonymity-and-youtubes-new-blurring-tool/>.
- . 2013. "Is This For Real? How InformaCam Improves Verification of Mobile Media Files." *WITNESS Blog*. Accessed January 20, 2015. blog.witness.org/2013/01/how-informacam-improves-verification-of-mobile-media-files/.
- . 2014. "About." Accessed January 7, 2014. <http://www3.witness.org/about-us>.
- . 2015. "About." Accessed July 18, 2015. <http://witness.org/about/>.
- Wokke, Arnoud. 2012. "OPTA waarschuwt overheidswebsites voor overtreden cookiewet." *Tweakers.net*, September 6. <https://tweakers.net/nieuws/84209/opta-waarschuwt-overheidswebsites-voor-overtreden-cookiewet.html>.
- Wood, David. 2003. "Foucault and Panopticism Revisited." *Surveillance & Society* 1 (3): 234–39. <http://www.surveillance-and-society.org/articles1%283%29/editorial.pdf>.
- Wood, Molly. 2014. "Privacy Please: Tools to Shield Your Smartphone." *The New York Times*, February 19. <http://www.nytimes.com/2014/02/20/technology/personaltech/privacy-please-tools-to-shield-your-smartphone-from-snoopers.html>.
- Wynne, Brian. 1996. "May the Sheep Safely Graze? A Reflexive View of the Expert-Lay Knowledge Divide." In *Risk, Environment and Modernity: Towards*

- a New Ecology*, edited by Scott Lash, Bronislaw Szerszynski, and Brian Wynne, 44–83. London.
- Zandbergen, Dorien. 2014. “‘Best Practice’ story telling on Smart Cities, and why we need better genres.” *The Last Resort: Critical and Creative Interventions in Today’s High-Tech Society*. November 18. <https://dorienzandbergen.nl/2014/11/18/best-practice-story-telling-on-smart-cities-and-why-we-need-better-genres/>.
- Zuiderveen Borgesius, Frederik. 2013. “Behavioral Targeting: A European Legal Perspective.” *IEEE Security & Privacy*, 11 (1): 82-85. doi: 10.1109/MSP.2013.5.
- . 2012. “Online Audience Buying.” *Unlike Utechnolos Conference*, Institute of Network Cultures March, 8-10 , Amsterdam, March 9. <http://vimeo.com/38840197>.
- Žižek, Slavoj. 2011. “Ethics of Consumption - cultural capitalism.” Accessed on August 27, 2015. <https://www.youtube.com/watch?v=GRvRm19UKdA>.

Surveillance awareness projects, organisations and software

- AdBlock. 2016. Accessed November 22. <https://getadblock.com/>.
- AdNauseam. 2016. Accessed November 22. <https://adnauseam.io/>.
- Cabledrum. 2016. Accessed November 22. <http://www.cabledrum.net/>.
- CameraV. 2016. Accessed November 22. <https://guardianproject.info/apps/camerav/>.
- Chaos Communication Congress. 2016. Accessed November 22. <https://events.ccc.de/>.
- Chaos Computer Club. 2016. Accessed November 22. <https://www.ccc.de/en/>.
- Cryptome. 2016. Accessed November 22. <https://cryptome.org/>.
- Cryptoparty. 2016. Accessed November 22. <https://www.cryptoparty.in/>.
- Disconnect. 2016. Accessed November 22. <https://disconnect.me/>.
- Exposing the Invisible. 2017. Accessed October 30. <https://exposingtheinvisible.org/>.
- Ghostery. 2016. Accessed November 22. <https://www.ghostery.com/>.
- Github. 2016. Accessed November 22. <https://github.com/>.
- Global Intelligence files. 2016. Accessed November 22. <https://wikileaks.org/the-gifiles.html>.
- GlobalLeaks. 2016. Accessed November 22. <https://www.globaleaks.org/>.
- Gnunet. 2016. Accessed November 22. <https://gnunet.org/>.
- Google alarm. 2016. Accessed November 22. <http://fffff.at/google-alarm/>.
- Meet my shadow. 2016. Accessed November 22. <https://myshadow.org/>.
- N-1. 2016. Accessed November 22. <https://wiki.p2pfoundation.net/Lorea>.
- Off-The-Record Messaging (OTR). 2016. Accessed November 22. https://en.wikipedia.org/wiki/Off-the-Record_Messaging.
- OHM2013: Obeserve. Hack. Make. July 31 - August 4. <https://ohm2013.org/>.
- Open Observatory of Network Interference. 2016. Accessed November 22. <https://ooni.torproject.org/>.
- Open whisper systems. 2016. Accessed November 22. <https://whispersystems.org/>.
- Pretty Good Privacy (PGP). 2016. Accessed November 22. https://en.wikipedia.org/wiki/Pretty_Good_Privacy.
- PLUSD The Public Library of US Diplomacy. Accessed November 22. <https://wikileaks.org/plusd/>.
- Prismbreak. 2016. Accessed November 22. <https://prism-break.org/>

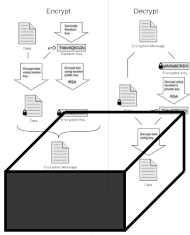
- en/.
- Privacy Cafes. 2016. Accessed November 22. <https://privacycafe.bof.nl/>.
- Privacy Guard. 2016. Accessed November 22. <http://www.androidcentral.com/cyanogen-os-privacy-guard-keeping-apps-seeing-your-data>.
- Privacy international. 2016. Accessed November 22. <https://privacyinternational.org/>.
- Project PM. 2016. Accessed November 22. <http://barrettbrown.blogspot.nl/2012/05/purpose-of-project-pm.html>.
- Retrosahre. 2016. Accessed November 22. <https://sourceforge.net/projects/retrosahre/>.
- Riseup. 2016. Accessed November 22. <https://riseup.net/>.
- Security in a box. 2016. Accessed November 22. <https://securityinabox.org/en>.
- ShareLab. 2016. Accessed November 22. <https://labs.rs/en/>.
- Spy Files. 2014. 15 September. Accessed November 22, 2016. <https://wikileaks.org/spyfiles/>.
- Telecomix. 2016. Accessed November 22. <https://telecomix.org/>.
- Tor. 2015. "Tor: Overview." Accessed January 20. <https://www.torproject.org/about/overview.html.en>.
- Transparency Toolkit. Accessed November 22. <https://icwatch.transparencytoolkit.org/>.
- WikiLeaks. 2016. "What is WikiLeaks." Accessed August 9. <https://wikileaks.org/What-is-Wikileaks.html>.



people and machines



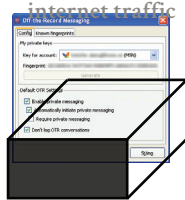
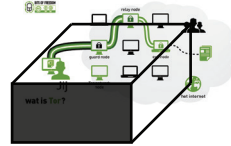
people and machines



E-mail

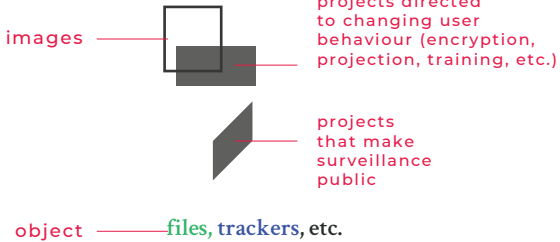
Account	Information
██████████	N/A
██████████	Last connection date: ██████████ this skills
██████████	Account created: ██████████ this skills

chat messages, audio and video



chat messages

How to read



trackers



trackers