Unfair Commercial Practices: an alternative approach to privacy protection

van Eijk, N.A.N.M.; Kannekens, E.; Hoofnagle, Chris Jay

Publication date
2017

Unfair Commercial Practices:

an alternative approach to privacy protection

Emilie Kannekens, Chris Hoofnagle and Nico van Eijk

Paper presented at the 2nd European edition of the Privacy Law Scholars Conference (PLSC-Europe), Tilburg, The Netherlands, 17 May 2017.

Amsterdam/Berkeley, 2017

Unfair Commercial Practices: an alternative approach to privacy protection

Emilie Kannekens[1], Chris Hoofnagle[2] and Nico van Eijk[3]

In the European Union, enforcement of privacy rules almost solely takes place by national enforcement authorities. They typically apply sector specific rules, based on the European Data Protection Directive. The responsibility primarily comes to the independent national data protection authorities. In the US, the Federal Trade Commission is the primary enforcer of privacy, using its power to prevent unfair and deceptive acts and practices. In this paper the American legal system will be discussed and compared to the European legal framework, which forms our finding that in the EU rules on unfair commercial practices could be enforced in a similar manner to protect people's privacy.[4] In the EU, the many frictions concerning the market /consumer-oriented use of personal data form a good reason to actually deal with these frictions in a market/consumer legal framework.

In this paper, we will first set forth how the US addresses privacy issues through application of the Federal Trade Commission's general power to prevent unfair and deceptive trade practices. Developed as a general tool to police business behavior, we explain how the FTC's authorities are applied in the privacy field with two examples. Particular attention will be given to the use of 'consent agreements': an instrument used by the Federal Trade Commission to bind violators of the rules of this supervisory authority to long lasting obligations under the risk of substantial—though rarely realized—financial penalties. Thereafter, the European framework of unfair commercial practices as set forth in the Unfair Commercial Practices Directive will be discussed. This article does not seek to give an exhaustive description of the US and European legal system; its aim is to give a first view of an alternative approach for privacy protection in the EU by an US example. Finally, in the analysis a comparison will be made between the

[1] Former research master student, Institute for Information Law (IViR, University of Amsterdam).
[2] Adjunct professor in the School of Law and the School of Information, University of California, Berkeley.
[3] Professor in Information Law, Institute for Information Law (IViR, University of Amsterdam).
[4] For this contribution, the term 'privacy' is used as an umbrella term to address both privacy in the traditional sense and privacy protection with regard to the storage and processing of (digital) personal data.

European and American legal frameworks. From this comparison, it will be clear that essential features of the frameworks correspond. Following from this, European rules regarding unfair commercial practices can be can be applied in a comparable manner.

The Authority to Prevent Unfair and Deceptive Commercial Acts and Practices in the US

For over a hundred years, The Federal Trade Commission (FTC) has been an independent federal agency acting to protect US consumers and businesses against unfair commercial practices. The FTC was founded a century ago as a response to the concerns regarding monopolies and trusts in the American marketplace.[5] Today, the FTC primarily concentrates on the prevention of anticompetitive business practices and consumer protection. In addition to the agency's general power to prevent unfair and deceptive practices, there are over 70 laws granting the FTC enforcement or administrative responsibilities.[6] The Federal Trade Commission Act (FTC act) from 1914 is the cornerstone which grants the FTC broad investigative powers against (potential) violators of the law and gives the FTC the task to write reports and recommendations for the American Congress. Although the FTC took on consumer cases since its founding, in 1938, the US Congress formally expanded the FTC's remit to address consumer protection. Section 5 of the FTC-act contains a broad, general prohibition on unfair and deceptive acts or practices:

> ***15 U.S. Code § 45 - Unfair methods of competition unlawful; prevention by Commission.***
>
> ***(a) Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade*** *(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.*

[5] C.J. Hoofnagle, *Federal Trade Commission, Privacy Law and Policy,* New York: Cambridge University Press, 2016 [Hoofnagle] p. 3.
[6] https://www.ftc.gov/enforcement/statutes

The broad interpretation of unfair and deceptive commercial practices in section 5 of the FTC-act is intentional. By not strictly defining what practices are considered unfair or deceptive, the FTC has the power to act against new unforeseen (technological) business practices. Over the years, clarification of the actual meaning these broad terms, has been shaped through policy rules, additional regulations and jurisprudence. Particularly the 1980 Unfairness and 1983 Deception policy statements have further defined the application of Section 5. In these statements the FTC summarized, partly based on rules developed in the jurisprudence, criteria for the examination of unfair or deceptive commercial practices. According to the FTC, a practice is deceptive when it meets the following three criteria:[7]

- *First, there must be a representation, omission or practice that is likely to mislead the consumer to her detriment.*
- *Second, we examine the practice from the perspective of a consumer acting reasonably in the circumstances. If the representation or practice affects or is directed primarily to a particular group, the Commission examines reasonableness from the perspective of that group*.
- *Third, the representation, omission, or practice must be a "material" one. The basic question is whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service*

Turning to unfair practices, the most relevant factor is whether a consumer has suffered injury. This perception derives from the pivotal S &H-case (1979) where the US Supreme Court decided that even though there was no competitive injury by a violation of antitrust law, the FTC had the power to protect the consumer against consumer injury on the basis of Section 5.[8] The 1980 policy statement sets forth when consumer injury is considered unfair. The requirement of “substantial injury to consumers” has been codified in the FTC-Act :

[7] Letter from Michael Pertschuk, Chairman, Fed. Trade Comm’n, et al., to Sen. Wendell H. Ford & Sen. John. C. Danforth (Dec. 17, 1980) (FTC Policy Statement on Unfairness).
[8] U.S Supreme Court, FTC v. Sperry & Hutchinson Co., 405 U.S. 233 (1972) (S & H).

To justify a finding of unfairness the injury must satisfy three tests:[9]

- *First of all, the injury must be substantial. The Commission is not concerned with trivial or merely speculative harms, and this includes claims of "emotional" injury*
- *Second, the injury must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces.*
- *Finally, the injury must be one which consumers could not reasonably have avoided*

Unfairness as a FTC power is politically controversial, and the above requirements represent Congressionally-imposed limits on unfairness. These limits came about because the FTC used unfairness entrepreneurially for decades, basing attacks on the cigarette industry, on shady funereal practices, on advertisers who made scientific claims regarding product efficacy, on used car salesmen who knew of defects in cars, and finally, on the idea that advertising to very-young children might be categorically "unfair" to them. Legal conservatives viewed such uses of the unfairness power as a kind of usurpation of legislative powers. Thus, Congress barred the FTC from basing unfairness interventions on policy or ethical rationales alone. As we will see below, the European unfairness framework is not hindered in this regard.

Privacy violation as an unfair or deceptive commercial practice

Since the early days of the internet the FTC has anticipated to the changing marketplace by protecting American consumers against unfair or deceptive commercial practices concerning their online privacy. Since 2002, the FTC has brought more than 130 spam and spyware cases and over 50 data security cases against small and large companies including Facebook, Google, Twitter and Microsoft.[10]

[9] 15 U.S.C. §45(n).
[10] Federal Trade Commission, Privacy & Data Security Update, 2015, p.2 & p. 4

Section 5 gives the FTC the primary legal authority to enforce privacy issues.[11] Section 5 is a powerful tool for this purpose, because the FTC forged a favorable body of caselaw in pursuing false advertising cases for a century.[12] The fact that many online companies offer their services free is not considered a legitimate ground to exclude these services from the obligations of Section 5. Neither does the FTC take a fundamental rights approach as the core for protecting privacy. Their perspective is economically oriented, aimed at the protection of the consumer: "*In all of its privacy works, the FTC's goals have remained constant: to protect consumers' personal information and ensure that consumers have the confidence to take advantage of the many benefits offered in the marketplace."*[13]

Most online privacy issues concern deceptive acts or practices: a representation, omission or practice that is likely to mislead the consumer.[14] For example, when the privacy policy of an online service omits essential information or contains false claims about how users' internet behavior is being monitored.[15] For act or practice to be deceptive, no substantial injury of the consumer needs to be proved—the deception need merely be "detrimental." Often this means that the mere fact that the consumer is misled by the information provided is sufficient to establish a violation, on the theory that the consumer may have chosen a competing service had the truth been known. By contrast, for an act to be unfair the consumer must have suffered injury. Complicating matters is that many argue that economic harm is necessary to establish "injury," yet privacy issues often lack an out-of-pocket monetary loss. Therefore, in the early 90's privacy cases were not seen as cases that could fit into the category of unfair commercial practices. The FTC has argued that privacy and security problems now nonetheless constitute substantial injuries, for instance when data breaches predispose consumers to identity theft or

[11] Furthermore, the FTC protects the privacy of consumers on the base of (sector)specific laws including the Children's Online Privacy Protection Act of 1998.
[12] Hoofnagle, p.146.
[13] Federal Trade Commission, Privacy & Data Security Update, 2015, p.1.
[14] Hoofnagle, p.160.
[15] Sears Holdings Mgmt. Corp., Docket No. C-4264, File No. 0823099, Federal Trade Commission, 9 September 2009, (Complain), p.5.

where data were sold despite promises not to.[16] Many in the industry dispute this idea and in a series of cases, companies have challenged the FTC's position, arguing that security breaches are not likely to cause or do not cause substantial injury.[17]

Enforcement of privacy issues by the FTC: consent agreements

There are no formal factors for matter selection by the FTC, although harm to consumers seems to be the leading consideration in allocation of enforcement resources. This determination is solely left to the discretion of the agency.[18] They can, on their own initiative, or following a consumer or complaint raised by a competitor, start an investigation of unfair or deceptive commercial practices. The FTC has broad investigative powers including subpoenas, access orders and the power to compel companies to file reports. However, the FTC has no general power to levy civil penalties. This lack of civil penalty authority reflects a concern for due process—because the FTC can determine what is "unfair" or "deceptive," it would seem iniquitous for it to define new proscriptions and fine companies for violating them. Penalties can only be imposed by the courts as a result of additional procedures by the FTC, or if the law specifically grants the power to the FTC to impose them.[19] Therefore many privacy cases result in a settlement between the respondent and the FTC. Because most of these cases settle, the precise contours of the FTC's power is not that well explored. For instance, recently, the 9th circuit held that the FTC, categorically, cannot police common carriers, even if the common carrier is engaging in non-common carriage activities.[20] Two cases currently in litigation, LabMD and D-Link fundamentally challenge the FTC's ability to take preventative action in security

[16]For example see: In the Matter of Gateway Learning Corp., FTC File No. 042 3047 (September 17, 2004) (company retroactively changed a privacy policy and sold customer's information on an opt-out basis; retroactive policy change and data sale was unavoidable, and in aggregate represented a substantial injury) .
[17] *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015); *LabMD, Inc., v. FTC*, No. 16-16270-D (11th Cir. 2016); *FTC v. D-Link Corp*., No. 3:17-cv-00039 (N.D. Cal. 2017).
[18] Hoofnagle, p.100.
[19] Such is the case in the COPPA. In 2006, the FTC imposed a 1 million dollar fine on the website Xanga.com for the processing of personal data of minors without their parents' consent. Also see: Chris Jay Hoofnagle, *Assessing the Federal Trade Commission's Privacy Assessments, 14(2) IEEE Security & Privacy* 58–64. (Mar/Apr. 2016), p.59.
[20] *FTC v. AT&T Mobility LLC*, No. 15-16585 (9th Cir. 2016).

cases because the defendants argue that consumers are “unlikely” to ever actually experience an injury.[21]

By a settlement, the decision is made final and the respondent waives his right to juridical process. These settlements, the so-called consent agreements mostly aim to achieve long-term behavior changes by the respondent. To illustrate the substance and the consequences of these agreements, we will now discuss two examples; the cases against Facebook and Google.

Unfair and Deceptive commercial practices: Google and Facebook[22]

In 2004 Google, already conquering the world with its search engine, became even more famous with the introduction of the new, free email service: Gmail. Not the email service itself was significantly different, the internal storage capacity offer of 1 gigabyte per user was. It had to be a joke; Gmail was launched on April 1st and at that time popular rival Windows Hotmail Service merely provided 2 megabytes of free storage. However, the offer proved to be true and users would never have to erase their emails again. Of course, the benefits were twofold. Because users no longer erased their information, they (on the base of the terms and conditions) agreed to have their information analyzed. Through analyzing these huge amounts of data, Google could improve its future services.

The same year Facebook started what would later become the world’s largest social network. As a result of the network effects Facebook grew fast, really fast. At the end of 2004 Facebook had 1 million users, in 2008 100 million and in February 2010 around 400 million.[23]

Google’s response to Facebook’s service was inevitable. In February 2010, the new service ‘Google Buzz’ was launched. Google Buzz allowed users to share extensive information with

[21] See supra footnote 18.

[22] The description in this section is partly based on the records of complaints to the FTC in both cases, for the full cases see: https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter and https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.

[23] Nowadays (2016) Facebook claims to have surpassed 1 billion users.

each other via public or private groups. To give the Buzz service an extra boost, Google used its Gmail users to populate the service. Before the service was activated, Gmail users were presented with a welcome screen with the question if they 'Sweet! Check out Buzz' wanted, or 'Nah, go to my inbox' did not want to use Google Buzz. Regardless of the user's choice, the service was activated.

Even though the service itself did not differ much from other already existing social media platforms, the launch of Google Buzz caused public outcry and opposition against the new service. In a similar manner to Facebook or Twitter, Google Buzz-users could be followed by or follow other users. For the convenience of the users, Google automatically generated these lists based on the email traffic of Gmail users. When a user created a profile the list would automatically, and without an explicit warning, become public. As a result of this process personal information (think of names and email addresses of lawyers, doctors or (ex-) lovers) were made public without explicit consent or even without the user's knowledge.

Besides Google, Facebook has also been criticized repeatedly for violating the privacy of its users. In 2007 Facebook started the new advertising feature 'Beacon', an application which tracked the internet behavior of users on Facebook-affiliated websites. When a user purchased an item on one of the affiliated websites, an automatic notification of the activity was published on the user's newsfeed, making it visible for all the Facebook user's friends. Many users weren't properly aware of the new service, which let to all sorts of awkward situations - from spoiling the surprise of Christmas presents to revealing embarrassing purchases.[24] The Beacon program was shut down from the social network in 2009. This same year, Facebook changed its privacy policy in order to, in its own words: "*give you more control of your information and help you stay connected'*. What Facebook did not mention clearly enough was that the existing privacy settings of its users were overridden by the new ones, making information, such as friend lists, profile pictures or Facebook groups from now on publicly visible. Facebook's new privacy clauses even attracted the attention and criticism of the US Senate.[25] Furthermore many users

[24] E. Nakashima, 'Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy' *The Washington Post*, 30 November 2007.
[25] C. Dwyer, 'Privacy in the Age of Google and Facebook', *IEEE T&S Magazine*, 13 September 2011, p.62

found it unclear to what extend Facebook shared information of its users with third parties. Facebook had repeatedly mentioned not to share this information with advertisers, nevertheless '*targeted advertisements'* appeared on user's newsfeeds. These advertisements are specifically selected for a user based on individual characteristics, for instance: age, location, sex, marital status and education.

In an investigation following a complaint, the FTC came to the conclusion that in the Google Buzz-case Google had acted deceptive in respect to its consumers. Firstly, Google explicitly informed its users in Gmail's privacy policy that personal data of Gmail users would only be used for the functioning of the email service. If Google would use the data for other purposes, it would ask for prior consent by the user. Contrary to these promises, Google used the data of Gmail users to support the Google Buzz service. Secondly, Google mislead its consumers by giving the impression that when they clicked the '*Nah, go to my inbox'*-button, the service would not be activated. Thirdly, Google had failed to demonstrate adequately that user had no control over the disclosure of personal information namely, the email-addresses and names of the people with whom they communicated with most. These practices were deceptive and therefore in breach of Section 5 FTC act.

From the investigation in the Facebook-case, the FTC announced that during the time period of 2007-2009, Facebook had violated the FTC-act seven times: six times by deceptive acts or practices and one time by unfair acts or practices. The misleading practices in the Facebook-case are comparable to the Google-case. Facebook also did not keep the promises in their privacy policy. For example, by selling personal information to marketers while promising not to do so. Furthermore, Facebook misled its consumers by using phrases like '*to give you more control',* when in reality this wasn't the truth, and by providing 'third party apps' with an 'Verified Apps' button. This 'Verified Apps' button could be purchased by the apps themselves for a payment to Facebook. The button had no connection to the security or confidentiality of the application. Furthermore, Facebook acted unfair when it retroactively changed its privacy policy in 2009 and disclosed prior collected information of its users by overriding the user's settings. According to the FTC, this caused the consumer injury.

Users with formerly invisible profiles could now receive unwanted contact form other users and pages which the user had previously shielded now revealed highly sensitive data to the public including their political or sexual preference.

Consent Agreements Google and Facebook

Both cases were settled in the form of a consent agreement between the respondent and the FTC.[26] These agreements are very compact and to the point. They exist of no more than approximately ten pages. Although the agreements are drafted according to the circumstances of the case, they to a large extent correspond with each other. The agreements are highly standardized (previous and later agreements of other cases contain similar terms). The agreements mainly cover agreements on data processing, internal compliance and reporting/disclosure requirements, as will be explained below.

Processing of data[27]

For the processing of personal data, the FTC orders the respondent to, in any manner, refrain from misrepresenting information, expressly or by implication, about a) (the purpose of) collecting, disclosing and processing information; b) the extent to which users have or may obtain control over this information ; c) the extent to which information is made available to third parties; d) the steps taken by the respondent to verify the privacy or security of third parties; e) the extent to which information is made accessible to third parties after the deletion or deactivation of a user's account; f) the extent to which the respondent complies with or participates in any privacy or security programs such as the U.S.-EU Safe Harbor Framework; g) the consequences of new forms of information sharing with third parties.

[26] https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf and https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf
[27] Summary/ description of paragraph I and II of the consent orders

Compliance[28]

For internal compliance, the FTC orders the respondent to implement and maintain a comprehensive privacy program that is designed to address privacy risks of new and existing products and services for consumers, and to protect the confidentiality of information. The program shall be appropriate to the size and complexity of the respondent's business and will include at least: a) the training of employees responsible for the privacy program; b) identification of the foreseeable risks that could result in the unauthorized collection or disclosure of information; c) implementation of reasonable privacy controls and procedures to address these risks, and regular testing or monitoring of the effectiveness of these controls and procedures; d) the respondent to take reasonable steps to select service providers capable of appropriate privacy protection, and by contract with the service provide require them to implement and maintain this protection; e) the evaluation and adjustment of the privacy program when changes or circumstances could impact the effectiveness of the program.

Assessments[29]

Both companies agreed upon obligations to provide substantial assessments and reports ('assessments'), proving their implementation of the privacy program and further compliance with the order. The initial assessment has to be completed within 180 days after the order and will continue on a 2-year base for 20 years. These assessments are to be completed by qualified, objective, independent third-party professionals with a minimum of 3 years of experience in the field of privacy and data protection. Furthermore the companies will make available upon request of the FTC: a)for a period of 3 years from the date of completion, the statements that describe how the respondent will maintain the privacy and confidentiality of information, and all the materials relied upon to make the statements; b) for a period of 6

[28] Summary/description of paragraph III (Google) and paragraph IV (Facebook) of the consent orders.
[29] Summary/description of paragraph IV and V (Google) and paragraph V and VI (Facebook) of the consent orders.

months after received, all consumer complaints received by the respondent about the unauthorized collection, use or disclosure of information; c)for a period of 5 year after received, all documents that contradict, qualify, or call into question respondent's compliance with this order; d) for a period of 3 years after preparation of the assessment, all material relied upon to prepare the assessment including reports, studies, training materials.

Consequences of the consent agreements

If a business continues to act unfair or deceptive after signing the consent agreements, the FTC can take the case to court to order for permanent injunctions and civil penalties. This happened to Google in 2012, when the FTC came to the conclusion that Google had placed cookies on user's computers without their knowledge. Google 'secretly' collected cookies from users of the Safari internet browser by overriding the Safari software that blocked these cookies. According to the FTC, unauthorized collection of information from user's web browsing activity was a violation of the agreement. The District Court of the Northern District of California approved upon the order to impose a penalty of no less than 22,5 million dollars; the record penalty for a violation of a FTC order at that time.[30]

When Facebook took over WhatsApp in 2014, the consent agreement between the FTC and Facebook caused the FTC to write an open letter to Facebook and WhatsApp.[31] In the letter the FTC expressed its concerns about compliance with the privacy promises that WhatApps made to its users. The director of the Bureau of Consumer Protection wrote: '*WhatsApp has made a number of promises about the limited nature of the data it collects, maintains, and shares with third parties -promises that exceed the protections currently promised to Facebook users.*' If WhatApp did not continue to honor these promises, both companies would violate Section 5 of the FTC act and Facebook would also break the promises of the consent agreement. According

[30] United States District Court for the Northern District of California, November 16, 2012, No. CV 12-04177 SI. For further information: C. Arthur, ' Google to pay record $22,5m fine to FTC over Safari tracking', *the Guardian,* 9 Augustus 2012 https://www.theguardian.com/technology/2012/aug/09/google-record-fine-ftc-safari
[31] https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf

to the FTC, both WhatsApp and Facebook took adequate measures to ensure the privacy of their users

Unfair commercial practices in the European Union

Since 2005, within the EU the rules on unfair commercial practices have been harmonized by the Unfair Commercial Practices Directive ('the Directive' or the UCPD).[32]

The Directive aims to harmonize the rules on unfair commercial practices in the member states on a far-reaching level through the measure of maximum harmonization. [33] As a result, the member states must implement only the rules as set forth in the directive. When a directive embodies a standard of minimum harmonization, the directive only sets forth a level of minimum protection and the member states remain free to provide a higher level of protection in their national laws. With maximum harmonization, both national laws that provide a lower level of protection and higher level of protection are not permitted.

This strict application of the Directive caused member states to substantially adapt their national legal systems in order to comply with the provisions of the Directive.[34] Not only is the Directive applicable to all business-to-consumer transactions, unless they are explicitly excluded, the Directive is also the leading instrument for these transactions. Excluded from the Directive are financial services and real-estate. Furthermore, it is specifically mentioned that article 13 sub 3 of the E-Privacy directive regarding unwanted communication (spam) should remain unaffected.[35] If the Directive is not excluded in sector specific EU-law, the rule of the *lex*

[32] Directive 2005/29/EC

[33]The first Report on the application of the UCPD contains a list of national provisions which have been declared 'general prohibitions' by the European Court of Justice due to their incompatibility with the maximum harmonization of the Directive. See: European Commission, COM (2013) 139 final, First Report on the application of Directive 2005/29/EC, p.6.

[34] Ibid, p.4.

[35] The Directive 2002/58 on Privacy and Electronic Communications (E-Privacy Directive) together with the General Data Protection Regulation form the main European legislative framework on data protection. The E-Privacy Directive was mainly drafted to address privacy concerns caused by new technologies. The Directive builds upon telecommunication laws and applies to electronic communication through public networks. In 2009, the Directive was revised and is now mostly known for its prior consent rules on the use of cookies. A new revision of the E-

speciales applies. This also applies to the Data Protection Directive. Therefore, both instruments can exist without prejudice.

Unfair commercial practices in the UCPD

Article 5 of the UCPD contains an exhaustive list of the possible grounds on which commercial practices are considered unfair. A commercial practice is unfair if: a) it is in contrary to the requirements of professional diligence and b) it materially distorts or is likely to distort the economic behavior of the average consumer.[36]

Misleading commercial practices and aggressive commercial practices are considered particularly unfair under article 5 of the Directive. In these cases, there is no need to investigate if the trader acted contrary to the requirements of professional diligence. However, the practice still needs affect the economic behavior of the average consumer.[37] Misleading practices are far out the most used ground on which unfair commercial practices are enforced on a national level.[38] Article 6 and 7 of the UCPD give a more detailed explanation of misleading practices. Misleading practices occur in particularly when the trader provides a) false information, deceptive representation or misleading omission, b) causing the average consumer c) to make a decision about a transaction which he would not have made otherwise. Aggressive commercial practices are according to article 8 and 9, practices that involve harassment, coercion or undue influence. Annex I of the Directive contains a 'black list'. The practices on this list are considered unfair, under all circumstances. Examples of practices on

Privacy Directive is currently in progress see: https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive .

[36] As such, the UCPD is less encumbered than the FTC approach. The FTC cannot use public policy—such as ethical concerns—as the primary basis for an unfairness action, whereas the UCPD explicitly allows professionalism norms to shape unfairness contours. In addition, the UCPD approach appears to be more autonomy oriented. While the FTC is focused on whether a business practice causes injury, the UCPD approach focuses on whether the practice might adversely affect consumer behavior.

[37] ECJ 16 April 2015, C-388/13 (Nemzeti Fogyasztóvédelmi Hatóság/UPC).

[38] European Commission, COM (2013) 139 final, First Report on the application of Directive 2005/29/EC, p.14.

the black list are: falsely describing a product as free or '*bait advertising'* (when the trader makes an attractive offer only with the purpose of selling a different product).

In other words, in order to determine whether a practice is prohibited, the Directive needs to be read backwards. The first thing to consider is if the practice is named on the black list. Thereafter, if the practice is either aggressive or misleading. Lastly, if the practice could fall under the open norm of article 5 sub 2, being contrary to the requirements of professional diligence.[39] It is left to the national enforcement agencies or juridical authorities to determine in each individual case, except for the practices on the black list which are always unfair, if a practice is unfair. For example, in the Netherlands unfair commercial practices fall under the open norms of general tort law.

Privacy and the UCPD

Within the European Union it seems that the UCPD is hardly used to enforce issues related to the privacy of the consumer.[40] Privacy enforcement almost entirely takes place on the base of sector specific privacy regulation, for instance, based on the Privacy Directive.[41] As previously mentioned, the UCPD has a very wide scope; it safeguards the interests of consumers in all business-to-consumer transactions, in all sectors. The European Court of Justice confirmed in the *Trento Sviluppo*-case that the applicability of the Directive goes beyond the concept of a

[39] R.W. de Vrey, Handelspraktijken en Reclame, in: E.H Hondius, G.J. Rijken, Handboek Consumentenrecht, Zutphen: uitgeverij Paris bv, 2015, p.385.

[40] For this study, the authors did not complete an exhaustive research, however an initial scan of the available literature and journals did not provide any recent information on the enforcement of privacy issues on the basis of the UCPD. With the exception of Germany, where unfair commercial practices have always received a remarkable amount of attention. In a recent ruling, the Bundesgerichtshof ruled that registration of default could be a unfair commercial practice. Furthermore, the Bundeskartellambt initiated an investigation into the anti-competitive aspects of a violation of privacy rules:
(http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2016/02_03_2016_Facebook.html)

[41] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive will be replaced by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).

'transaction' as being the purchase of a product in a store.[42] Furthermore, the European Commission stated in its guidance document on the implementation/application of the Directive that privacy issues could simultaneously result into a violation of data protection law and a violation of unfair commercial practices law. This could especially be the case when a trader is not transparent about its commercial practices.[43] The Commission states: '*Under Articles 6 and 7 of the UCPD, traders should not mislead consumers on aspects that are likely to have an impact on their transactional decisions. More specifically, Article 7(2) and No 22 of Annex I prevent traders from hiding the commercial intent behind the commercial practice*.'[44]

Enforcement of Unfair Commercial Practices in the EU

The enforcement of unfair commercial practices remains mostly harmonized, Article 11 of the UCPD states that the member states *'Shall ensure that adequate and effective means exist to combat unfair commercial practices',* and that persons or organizations should be able to combat such practices by taking legal action and/or bringing the case before administrative authorities. Except from these rules, it is up to the member states to decide if unfair commercial practices can be battled through public or private procedures, or both. It is also predominantly left to the member states to decide which sanctions apply to violator of the Directive. Only article 13 requires that the member states lay down penalties for infringement of national provisions adopted in application of the Directive and that these penalties shall be *'effective, proportionate and dissuasive'.*

[42] *ECJ, 1*9 December 2013, C-281/12 (*Trento Sviluppo)* par. 36.
[43] European Commission, COM (2016) 163 final, Guidance on the application of the Unfair Commercial Practices Directive, p.27.
[44] Ibid. Article 7.2 reads: 'It shall also be regarded as a misleading omission when, taking account of the matters described in paragraph 1, a trader hides or provides in an unclear, unintelligible, ambiguous or untimely manner such material information as referred to in that paragraph or fails to identify the commercial intent of the commercial practice if not already apparent from the context, and where, in either case, this causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.' No 22: 'Falsely claiming or creating the impression that the trader is not acting for purposes relating to his trade, business, craft or profession, or falsely representing oneself as a consumer.

Analysis and Conclusion

In the previous paragraphs, we have set forth the doctrine of unfair commercial practices and its applicability to the enforcement of privacy rules from both the European and American perspective. In the United States, there appears to be a close link between unfair commercial practices and privacy enforcement. The long history of the FTC and the lack of an 'omnibus bill', such as a Federal Privacy Regulation, both played a part in this development. On the contrary, in the European Union the field of unfair commercial practices and privacy regulation have developed separately. Consumer and privacy laws are based on a different normative framework, elaborated in different directives and know different national enforcement procedures and authorities.

The FTC enforces a prohibition on unfair commercial practices on the base of two grounds: unfair acts or practices and deceptive acts or practices. For an act to be unfair, substantial injury is required. In the UCPD unfair commercial practices can fall under the open norm of article 5 sub 2, aggressive practises and the prohibited practices on the black list. This black list particularly illustrates the different legislative approach of jurisdictions. Section 5 of the FTC-act does not contain any practices that are considered unfair without a normative test.

The FTC enforces most of its privacy cases on the base of a prohibition on deceptive practices under Section 5. The prohibition as laid down by the FTC, shows obvious similarities with the prohibition on misleading practices under article 6 and 7 of the UCPD. The terminology used might not be identical. However, the criteria correspond to a large extent, as can be seen in the following table.[45]

[45] In a next version of this paper, we will further detail the comparison between the US and EU regulatory framework.

Comparison FTC-Act/PCPD[46]	
FTC Act	**UCPD**
Criteria deception: 1. *Mislead* There must be a representation, omission or practice that is likely to mislead the consumer 2. *Reasonable consumer:* From the perspective of a consumer acting reasonably in the circumstances. 3. *Material:* The act or practice is likely to affect the consumer's conduct or decision with regard to a product or service.	**Misleading commercial practices:** *1. Mislead* The practice deceives or is likely to deceive through the information it contains or the deceptive presentation thereof, including omission. 2.*Average consumer:* Reasonably well-informed and reasonably observant 3.*Transactional decision:* If the misleading practice causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.

As mentioned before, when the FTC enforces a privacy case concerning unfair or deceptive commercial practises, it does not have individual civil penalty authority. Within the US legal framework, the FTC has to refer the matter to court in order to impose such sanctions. However, if the FTC finds that a law violation has occurred, this generally leads to a 'consent agreement'. Such an agreement is focused on accomplishing behavioural change by the violator, rather than direct punishment. If the agreement is not respected, the FTC will turn to court for a penalty. These penalties can be substantial in size.

In Europe, compliance and enforcement of privacy rules primarily relies on sector-specific rules set out in the Privacy Directive (to be replaced by the new privacy regulation). However, it should be remarked that partly due to lack of competence and experience, actual enforcement

[46] The schedule is constructed from the FTC Policy Statement on Deception, the UCP Directive and the first European Commission report on the functioning of the Directive UCP.

in practice has been limited. The same applies to the Unfair Commercial Practices Directive (UCPD) as the leading instrument with regard to relations between suppliers of goods / services and consumers. The application of the UCPD in privacy issues is insignificant, even though business-to-consumer relations are becoming of increasing importance. The collection and processing of personal data is in today's information society is mainly used for transactional purposes: to realise the sale of a product or to provide a service. The European directive on unfair commercial practices leaves it to Member States to ensure an effective enforcement system.

As can be noted from the table above, there is remarkable material similarity between the American and the European regulatory framework on deceptive/unfair commercial practices. The conceptual frameworks overlap and in both cases the concept of consumer protection is key. There are no barriers to also apply the doctrine of unfair business practices in Europe in the context of privacy enforcement. The rules of the UCPD can be applied as a general regulatory framework where the collection or processing of personal data within a business-to-consumer relationship falls within the scope of the Directive.

There are numerous reasons to choose for a more market-consumer based approach in today's information society. The collection and processing of (personal) date is often described as 'the new oil', the new driving force of the digital economy.[47] Misconduct in the context of privacy and the collection/processing of personal data is primarily motivated by economic motives, not by an attempt to violate fundamental rights, the second is more a consequence of the first.[48] This should be considered for compliance and enforcement which should, in the first place, be consumer oriented.

From our perspective, 'soft' privacy cases (issues which mostly concern market behavior) should be solved through market-oriented regulation. In this scenario, European market and consumer authorities should play a more active role, whether or not in consultation with data

[47] For example, in the speech of former EU Commissioner Kroes: http://europa.eu/rapid/press-release_SPEECH-12-149_en.htm.

[48] We are not trying to state that fundamental rights are less important. On the contrary, fundamental rights are of such value that –unlike unfair business practices- you can't put a price tag on them.

protection authorities. It is, after all, their task to speak up for the market and consumer interests.[49] Through applying rules on unfair commercial practices, the enforcement of privacy issues could become more effective. However, effective enforcement should not solely rely on the ability to impose fines, but should also focus on prevention and behavioral change. To achieve this, European supervisory authorities could follow the example of the FTC's consignment agreements by entering into binding agreements between the authority and a private party.[50]

[49] Recently the European Commission asked social media companies to comply with EU consumer rules (IP/17/631, Brussels, 13 March 2017). The press release mainly refers to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993), but also mentions the UCP. This Council Directive is also mentioned in recital 42 of the GDPR.

[50] It should be noted that a similar instrument of 'binding commitments' exists in European competition law (article 9 of the Council Regulation (EC) No 1/2003). Also see the proposal to Proposal for a Directive 'to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market' (Brussels, 22 March 2017 COM(2017) 142 final). Furthermore, the EDPS emphasized the need for more regulatory cooperation in its opinion 8/2016 'on coherent enforcement of fundamental rights in the age of big data' (Brussels, 23 September 2016). This opinion is more or less a follow up on it earlier preliminary opinion on 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy (March 2014).