1-1-2017

Unfair Commercial Practices: A Complementary Approach to Privacy Protection

Nico van Eijk

Chris Jay Hoofnagle
Berkeley Law

Emilie Kannekens

Unfair Commercial Practices:

A Complementary Approach to Privacy Protection

*Nico van Eijk, Chris Jay Hoofnagle and Emilie Kannekens**

Millions of European internet users access online platforms where their personal data is being collected, processed, analysed or sold. The existence of some of the largest online platforms is entirely based on data driven business models. In the European Union, the protection of personal data is considered a fundamental right. Under Article 8(3) of the EU Charter of Fundamental Rights, compliance with data protection rules should be subject to control by an independent authority. In the EU, enforcement of privacy rules almost solely takes place by the national data protection authorities. They typically apply sector-specific rules, based on the EU Data Protection Directive.[1] *In the United States, the Federal Trade Commission is the primary enforcer of consumers' (online) privacy interests. The agency's competence is not based on the protection of fundamental rights, but on the basis that maintenance of a competitive, fair marketplace will provide the right choices for consumers to take. In this Article the US legal framework will be discussed and compared to the EU 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.*[2] *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.*

We will first set forth how the United States (US) addresses privacy issues through application of the Federal Trade Commission's (FTC) general power to prevent unfair and deceptive trade practices. Developed as a general tool to police business behaviour, 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 FTC to bind violators of unfair and deceptive trade practices laws to supervisory authority, long lasting obligations under the risk of substantial—though rarely realised—financial penalties. Thereafter, the European Union (EU) 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 EU legal system; its aim is to give a first view of a complementary approach for privacy protection in the EU by a US example. Finally, in the analysis a first compari-

DOI: 10.21552/edpl/2017/3/7

* Nico van Eijk, Professor in Information Law, Institute for Information Law (IViR), University of Amsterdam. Chris Jay Hoofnagle, Adjunct professor in the School of Law and the School of Information, University of California, Berkeley. Emilie Kannekens, Former research master student, Institute for Information Law (IViR), University of Amsterdam. For correspondence: <n.a.n.m.vaneijk@uva.nl>.

This article is based on a paper presented at the 2nd European edition of the Privacy Law Scholars Conference (PLSC-Europe), Tilburg, The Netherlands, 17 May 2017. The authors want to thank all those who shared their ideas and contributed to improving our project.

1 To be replaced (as of 25 May 2018) by the General Data Protection Regulation [GDPR, Regulation (EU) 2016/679]. For the purpose of this article, there is no relevant difference between the present and future regulatory situation.

2 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.

son will be made between the EU and US legal frameworks. From this comparison, it will be clear that essential features of the frameworks correspond. Following from this, we claim that EU rules regarding unfair commercial practices can be can be applied in a comparable manner.

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

For over a century, the FTC has been an independent federal agency acting to protect US consumers and businesses against unfair commercial practices. The FTC was originally founded as a response to the concerns regarding monopolies and trusts in the US marketplace.[3] Today, the FTC primarily concentrates on competition policy and consumer protection. In the consumer protection field, it generally does not regulate or supervise industries. Instead, it encourages firms to adopt privacy policies and to abide by the promises made in them. If violations of these policies are found, the FTC brings enforcement actions to subject the wrongdoer to supervisory oversight, thereby providing a deterrent effect on other firms in the field. These cases are motivated by consumer protection rights only indirectly. The FTC's main mission is to ensure fair competition, which is thought to create an environment respectful of consumer preferences. This leap from competition to a fair marketplace is a source of theoretical and practical tension because information markets differ from markets for ordinary products.[4]

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.[5] 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 US 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.

The broad, vaguely-defined mandate to prevent 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.[6] In these statements the FTC summarised, partly based on rules developed in the jurisprudence, criteria for the examination of unfair or deceptive commercial practices.

The legal theories of unfair or deceptive practices exist independently of each other. An act can either be deceptive, unfair or both, depending on the factual circumstances.[7] According to the FTC, a practice is deceptive when it meets the following three criteria:[8]

- 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

3 Chris Jay Hoofnagle, *Federal Trade Commission, Privacy Law and Policy* (Cambridge University Press 2016) 3.

4 Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54(2) Journal of Economic Literature 442–492.

5 Federal Trade Commission, 'Statutes Enforced or Administered by the Commission' <https://www.ftc.gov/enforcement/statutes>accessed 26 September 2017.

6 Letter from Michael Pertschuk, Chairman, Fed Trade Comm'n et al, to Sen Wendell H Ford and Sen John C Danforth (17 December 1980) (FTC Policy Statement on Unfairness).
Letter from James C. Miller III, FTC Chairman, to John D Dingell, Chairman, House Comm on Energy and Commerce 5–6 (14 October 1983) (FTC Policy Statement on Deception).

7 Hoofnagle, *Federal Trade Commission, Privacy Law and Policy* (n 4) 130.

8 FTC Policy Statement on Unfairness (n 7).

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. The FTC's power derives from the pivotal *S&H* case (1972) 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.[9] 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.[10] As elaborated in the Unfairness Statement, the FTC evaluates injuries with a three-part inquiry:
- 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 an FTC power is politically controversial. In fact, Congress explicitly barred the FTC from using public policy concerns (instead of consumer injury) as the lead basis for an unfairness action.[11] Limits on unfairness came about because the FTC used unfairness entrepreneurially for decades, making attacks on the cigarette industry,[12] on shady funeral practices, on advertisers who made scientific claims regarding product efficacy, on used-car salesmen who knew of defects in cars that they sold to unwitting buyers, 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, and the FTC has more broadly been under attack by those sceptical of the idea of an administrative state.[13] Thus, Congress limited the unfairness authority by specifying that the FTC 'may consider established public policies as evidence to be considered with all other evidence [of injury]. Such public policy considerations may not serve as a primary basis for such determination.'[14] As we will see below, the EU unfairness framework is not hindered in this regard.

II. Privacy Violation as an Unfair or Deceptive Commercial Practice

Since the early days of the internet the FTC has reacted to the changing marketplace by protecting US 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.[15] The US regulates privacy through sector-specific statutes, but lacks a privacy law of general application. In the absence of general privacy protection, Section 5 has served as a kind of baseline consumer privacy law for Americans.

Section 5 gives the FTC the primary legal authority to enforce consumer privacy interests, so long as business activity constitutes deceptive or unfair trade practices.[16] Section 5 is a powerful tool for this purpose, because the FTC forged a favourable body of

9 US Supreme Court, *FTC v Sperry & Hutchinson Co*, 405 US 233 (1972) (*S & H*).

10 15 USC §45(n).

11 ibid.

12 As a reaction to the Surgeon General's finding that cigarettes caused cancer, the FTC mandated a rule requiring tobacco products to warn consumers of 'death from cancer.' Congress intervened and blocked the warning. Norman I Silber, 'With All Deliberate Speed: The Life of Philip Elman' (University of Michigan Press 2004).

13 Hoofnagle, *Federal Trade Commission, Privacy Law and Policy* (n 4) 57–66; Thomas O Mcgarity, *Freedom To Harm: The Lasting Legacy Of The Laissez-Faire Revival* (Yale University Press 2013); William J Baer, 'At the Turning Point: The Commission in 1978' in Patrick E Murphy and William L Wilkie (eds), *Marketing and Advertising Regulation: The Federal Trade Commission in the 1990s* (Univ of Notre Dame Press 1990); Michael Pertschuk, *Revolt Against Regulation: The Rise and Pause of the Consumer Movement* (University of California Press 1982).

14 15 USC 45(n).

15 Federal Trade Commission, 'Privacy & Data Security Update (2015)' (January 2016) 2, 4 <https://www.ftc.gov/reports/privacy-data-security-update-2015> accessed 27 September 2017.

16 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.

case-law in pursuing false advertising cases for a century.[17]

The FTC does not take a fundamental rights approach as the core for protecting privacy. Its perspective is economically oriented, aimed at the protection of the consumer through competition and a fair marketplace:

> 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.[18]

Most online privacy issues concern deceptive acts or practices: a representation, omission or practice that is likely to mislead the consumer.[19] The FTC may initiate a case against a company when the privacy policy of an online service omits essential information or contains false claims about how users' internet behaviour is being monitored.[20] For an act or practice to fall within the scope of the legal theory of deceptiveness, no substantial injury to the consumer needs to be proved—the deception need merely cause 'detriment.' Often this means that the mere fact that the consumer is misled by the information provided is sufficient to establish a violation, as the Deception Statement assumes that had the truth been known, the consumer would have chosen differently.

Recall that deception and unfairness are different theories. 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 1990s 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 where data were sold despite promises not to, the FTC declares that consumers have suffered or are likely to suffer substantial injury.[21]

The contours of the FTC Act are unclear, because Congress gave the agency a broad mandate, but also because the FTC typically does not explain why a practice is deceptive or unfair in great detail. Few companies challenge the FTC in court, and so there are few modern court opinions defining the agency's authority. Instead, the wrongness of the corporate act is simply declared in a complaint and consent decree agreed to by the respondent company. This is somewhat unsatisfactory and problematic. Concerns about vague powers and the level of due process afforded to respondent companies has sparked an FTC backlash. Now, in a series of cases, companies have challenged the FTC's interpretations of unfairness, arguing that security breaches are not likely to cause or do not cause substantial injury.[22]

III. 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.[23] The FTC can, on its 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.

17 Hoofnagle, *Federal Trade Commission, Privacy Law and Policy* (n 4) 146.

18 Federal Trade Commission, 'Privacy & Data Security Update (2015)' (n 16) 1.

19 Hoofnagle, *Federal Trade Commission, Privacy Law and Policy* (n 4) 160.

20 Sears Holdings Mgmt Corp, Docket No C-4264, File No 0823099, Federal Trade Commission, 9 September 2009, (Complain) 5.

21 For example see: In the Matter of Gateway Learning Corp, FTC File No 042 3047 (17 September 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).

22 *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 (ND Cal 2017).

23 Hoofnagle, *Federal Trade Commission, Privacy Law and Policy* (n 4) 100.

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.[24] Therefore many privacy cases result in a settlement between the respondent and the FTC. As explained above, because most of these cases settle, the precise contours of the FTC's power is not that well explored. For instance, recently, the US Court of Appeals for the Ninth Circuit held that the FTC, categorically, cannot police common carriers, even if the common carrier is engaging in non-common carriage activities.[25]

Two cases currently in litigation, *LabMD* and *D-Link*, challenge FTC authority by arguing that consumers are 'unlikely' to ever actually experience an injury.[26] In *LabMD*, a patient file appeared on a file-sharing network, yet there is no definitive evidence that the file was used to harm LabMD's patients. Similarly, in *D-Link*, the FTC alleged that the company's cameras and other devices were woefully insecure, but the agency did not document an example of the insecurity contributing to injury of a specific individual. If successful, these challenges will fundamentally change the FTC's ability to take preventative action to protect consumers whose privacy or security posture has been weakened, but not yet compromised.

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 behaviour changes by the respondent. Consent agreements are viewed as a contract and to be enforced, the FTC must bring suit. Despite the fact that a company engaged in wrongful practices and is under suspicion for continued noncompliance, the FTC bears the burden to show non-compliance. In some circuits, courts have put the burden on the FTC to show that the company engaged in *substantial* noncompliance—not a mere technical violation of the order.

To illustrate the substance and the consequences of these agreements, we will now discuss two examples; the cases against Facebook and Google.

IV. Unfair and Deceptive Commercial Practices: Google and Facebook[27]

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'. The email service itself was not groundbreaking. The internal storage capacity offer of 1 gigabyte per user, however, was. For instance, Google's popular rival Windows Hotmail Service at that time merely provided 2 megabytes of free storage. With Gmail, users would never have to erase their emails again. Of course the users' benefits of the service were also beneficial for Google. Because users no longer erased their information, Google could analyse the content, context, and metadata of their conversations, and at least one court has held that this was done without consent.[28] Through analysing 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 exponentially. At the end of 2004, Facebook had 1 million users, in 2008 - 100 million and in February 2010 - around 400 million.[29]

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 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 giving them the choice to tick the box: 'Sweet! Check out Buzz' or

24 Such is the case in the COPPA. In 2006, the FTC imposed a $1 million 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' (March/April 2016) 14(2) IEEE Security & Privacy 58–64, 59.

25 *FTC v AT&T Mobility LLC*, No 15-16585 (9th Cir 2016).

26 Hoofnagle, *Federal Trade Commission, Privacy Law and Policy* (n 4) 146.

27 The description in this section is partly based on the records of complaints to the FTC in both cases, for the full case reports see: Federal Trade Commission, 'In the Matter of Google Inc., a corporation' (24 October 2011) FTC Matter/File Number: 102 3136 <https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter> accessed 27 September 2017; Federal Trade Commission, 'In the Matter of Facebook Inc' (10 August 2012) FTC Matter/File Number: 092 3184 <https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc> accessed 27 September 2017.

28 In re: Google Inc. Gmail Litigation, 13-MD-02430-LHK (ND Cal 26 September 2013).

29 Nowadays (2016) Facebook claims to have surpassed 1 billion users.

'Nah, go to my inbox'. Regardless of the user's explicit consent, the service was activated. [30]

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.[31]

Besides Google, Facebook has also been criticised repeatedly for violating the privacy of its users. In 2007, Facebook started the new advertising feature 'Beacon,' an application which tracked the internet behaviour 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 were not properly aware of the new service, which led to all sorts of awkward situations - from spoiling the surprise of Christmas presents to revealing embarrassing purchases.[32] The Beacon programme 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.[33] Furthermore, many users 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 deceptively in respect to its consumers. Firstly, Google had informed its users, expressly or by implication, 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.[34] 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.[35] Thirdly, Google had failed to demonstrate adequately that users had no control over the disclosure of personal information namely, the email addresses and names of the people with whom they communicated with most.[36] The FTC concluded in its complaint that these false and misleading acts constituted deceptive acts or practices in breach of Section 5 FTC Act.[37]

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 neither kept the promises in their privacy policy. For instance, by selling personal information to marketers while promising not to do so or by misleading consumers through using phrases like 'Facebook's new, simplified privacy settings give you more control over the information you share,' while in reality users could no longer restrict access to personal information including friend lists. Furthermore, Facebook acted unfairly

30 'In the Matter of Google Inc., a corporation' (n 28) Complaint, 3 and Exhibit A.

31 Miguel Helft, 'Critics Say Google Invades Privacy With New Service' *The New York Times* (12 February 2010).

32 Ellen Nakashima, 'Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy' *The Washington Post* (30 November 2007).

33 Catherine Dwyer, 'Privacy in the Age of Google and Facebook' *IEEE T&S Magazine* (13 September 2011) 62.

34 'In the Matter of Google Inc., a corporation' (n 28) Complaint, 3, para16.

35 ibid para 17.

36 ibid para 18.

37 ibid para 26.

when it retroactively changed its privacy policy in 2009 and disclosed sensitive personal information of its users that Facebook previously had promised to keep private.[38] According to the FTC, this had caused or was likely to cause consumers substantial 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.

1. Consent Agreements Google and Facebook

The FTC investigations against Google and Facebook were both settled in the form of a consent agreement between the respondent and the FTC.[39] The consent agreements are very compact and to the point. They consist 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 standardised (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.

2. Processing of Data[40]

For the processing of personal data, the FTC ordered 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 US-EU Safe Harbour Framework; and g) the consequences of new forms of information sharing with third parties.

3. Compliance[41]

For internal compliance, the FTC ordered the respondent to implement and maintain a comprehensive privacy programme that is designed to address privacy risks of new and existing products and services for consumers, and to protect the confidentiality of information. The programme 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 programme; b) identification of the foreseeable risks that could result in the unauthorised 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; and e) the evaluation and adjustment of the privacy programme when changes or circumstances could impact the effectiveness of the programme.

4. Assessments[42]

Both companies agreed upon obligations to provide substantial assessments and reports ('assessments'), proving their implementation of the privacy programme and further compliance with the order. The initial assessment had to be completed within 180 days after the order and continued on a 2-year base

38 'In the Matter of Facebook Inc' (n 28) Compliant, para 29.

39 Federal Trade Commission, 'In the Matter of Google Inc., a corporation, Agreement Containing Consent Order' (2011) <https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf> accessed 27 September 2017 and Federal Trade Commission, 'In the Matter of Facebook Inc. Decision and Order' (27 July 2012) <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf> accessed 27 September 2017.

40 Summary/ description of paras I and II of the consent orders (ibid).

41 Summary/description of para III (Google) and paragraph IV (Facebook) of the consent orders (ibid).

42 Summary/description of paras IV and V (Google) and paragraph V and VI (Facebook) of the consent orders (ibid).

for 20 years. These assessments had 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 had to 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 months after received, all consumer complaints received by the respondent about the unauthorised 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; and d) for a period of 3 years after preparation of the assessment, all material relied upon to prepare the assessment including reports, studies, and training materials.

5. Consequences of the Consent Agreements

If a business continues to act unfairly or deceptively 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 users' 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, unauthorised collection of information from users' 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; the record penalty for a violation of an FTC order at that time.[43]

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.[44] In the letter the FTC expressed its concerns about compliance with the privacy promises that WhatsApp 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 WhatsApp did not continue to honour these promises, both companies could be in violation of Section 5 of the FTC Act and break the promises of the consent agreement. According to the FTC, both WhatsApp and Facebook took adequate measures to ensure the privacy of their users.

V. Unfair Commercial Practices in the European Union

Since 2005, within the EU the rules on unfair commercial practices have been harmonised by the Unfair Commercial Practices Directive (the Directive or the UCPD).[45]

The Directive aims to harmonise the rules on unfair commercial practices in the Member States on a far-reaching level through the measure of maximum harmonisation.[46] This strict application of the Directive has caused Member States to substantially adapt their national legal systems to comply with the provisions of the Directive.[47] The Directive is applicable to all business-to-consumer transactions, unless they are explicitly excluded from the Directive's scope. Excluded from the Directive are financial services, real-estate, and it is specifically mentioned that Article 13(3) of

43 United States District Court for the Northern District of California, 16 November 2012, No CV 12-04177 SI. For further information: Charles Arthur, 'Google to pay record $22,5m fine to FTC over Safari tracking' *The Guardian* (9 August 2012) <https://www.theguardian.com/technology/2012/aug/09/google-record-fine-ftc-safari> accessed 27 September 2017.

44 Letter from Jessica L Rich, Office of the Director, Bureau of Consumer Protection to Erin Egan, Chief Privacy Officer, Facebook, Inc and Anne Hoge, General Counsel, WhatsApp Inc (10 April 2014) <https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf> accessed 27 September 2017.

45 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No. 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') [2005] OJ L 149/22.

46 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, 'First Report on the application of Directive 2005/29/EC' (2013) COM (2013) 139 final, 6.

47 ibid 4.

the E-Privacy Directive regarding unwanted communication (spam) should remain unaffected.[48] If the application of the Directive is not excluded in sector-specific EU law, the rule of the *lex speciales* applies.[49] This also applies to the Data Protection Directive. Therefore, both instruments can exist without prejudice.

1. Unfair Commercial Practices in the UCPD

The UCPD follows a layered structure. It starts with a central general clause in Article 5(2), containing two cumulative criteria for unfair commercial practices.[50] 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 behaviour of the average consumer.[51]

The UCPD continues with two precise categories of unfair commercial practices in Article 5(4): misleading commercial practices and aggressive commercial practices. Misleading practices are by far the most-used ground on which unfair commercial practices are enforced on a national level.[52] Articles 6 and 7 of the UCPD cover criteria under which the consumer is likely to be deceived, including criteria for misleading omissions.[53] Misleading actions in general occur when the trader provides i) false information, deceptive representation or misleading omission, ii) causing the average consumer iii) to make a decision about a transaction which he would not have made otherwise.[54] Criteria for aggressive commercial practices are set forth in Articles 8 and 9. These practices involve harassment, coercion, physical force or more inconspicuous forms of undue influence including exploitation of vulnerability.[55]

The general clause and the two categories of unfair commercial practices are complemented by a blacklist in Annex I of the Directive. Unlike other practices, which have to be ascertained concretely, the practices on this list are considered unfair irrespective of the circumstances.[56]

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 falls under the blacklist in Annex I and is therefore immediately prohibited. Thereafter, if the factual circumstances of the practice fit within the general clauses of aggressive or misleading. Lastly, if the practice could fall under Article 5(2), being contrary to the requirements of professional diligence.[57] The general clause of Article 5(2) should function as a safety net for practices that do not fall under the more specific Articles of the Directive and should therefore be broad enough to be "future proof".[58] It is left to the national enforcement agencies or judicial authorities to determine in each individual case, except for the practices on the blacklist, if a practice is unfair under the requirements of the UCPD and criteria of the general clauses.[59] For example, in the Netherlands unfair commercial practices fall under the open norms of general tort law.

48 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 proposal to replace the Directive by a new Regulation is under discussion: <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation> accessed 27 September 2017.

49 Willem van Boom, Amandine Garde and Orkun Akseli, *The European Unfair Commercial Practices Directive – Impact, Enforcement Strategies and National Legal Systems* (Routledge 2014) 10.

50 Asterios Pliakos and Georgios Anagnostaras, 'Harmonising national laws on commercial practices: sales promotions and the impact on business to business relations' (2010) 35(3), European Law Review 425.

51 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 behaviour.

52 European Commission, 'Guidance on the implementation/application of Directive 2005/29/EC on Unfair Commercial Practices' (2016) COM (2016) 320 final, 58.

53 ibid.

54 art 6 (1) UCPD.

55 Van Boom, Garde and Akseli (n 50) 3.

56 Examples of practices on the blacklist are: Annex I (20) falsely describing a product as free or Annex I (5) when the trader makes an attractive offer only with the purpose of selling a different product (*bait advertising*).

57 RW de Vrey, 'Handelspraktijken en Reclame' in EH Hondius and GJ Rijken (eds), *Handboek Consumentenrecht*, (Uitgeverij Paris bv 2015) 385.

58 Commission, 'Guidance on the implementation/application of Directive 2005/29/EC' (n 53) 55.

59 Georgios Anagnostaras and Asterios Pliakos, 'Delimiting the harmonisation scope of the Unfair Commercial Practices Directive: towards a specific competitive intent requirement?' (2014) 39(5) European Law Review 701.

2. Privacy and the UCPD

Within the EU it seems that the UCPD is hardly used to enforce issues related to the privacy of the consumer.[60] Privacy enforcement almost entirely takes place on the basis of sector-specific privacy regulation, for instance, based on the Data Protection Directive.[61] 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. Considering that personal data is often sold to third parties and de facto has economic value, it is reasonable to assume that data-driven businesses engage in business-to-consumer transactions that would fall under the scope of the UCPD.[62] The European Commission has stated in its guidance document on the implementation/application of the UCPD that privacy issues could simultaneously result in a violation of data protection law and a violation of unfair commercial practices law. Especially when a trader is not transparent about its commercial practices.[63] The Commission stated:

> 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.[64]

Article 7 of the UCPD has a strong overlap with the Articles 13 ('Information to be provided where personal data are collected from the data subject') and 14 ('Information to be provided where personal data have not been obtained from the data subject') of the GDPR dealing with informing data subjects.

3. Enforcement of Unfair Commercial Practices in the EU

The enforcement of unfair commercial practices remains mostly unharmonised. Article 11 of the UCPD states that the Member States '[s]hall ensure that adequate and effective means exist to combat unfair commercial practices," and that persons or organisations should be able to combat such practices by taking legal action and/or bringing the case before administrative authorities. It is up to the Member States to decide if unfair commercial practices can be challenged through public or private procedures, or both. It is also largely left to the Member States to decide what sanctions apply to violators of the Directive. Article 13 only 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'. This procedural autonomy has led to different national enforcements styles across the EU.[65]

VI. Analysis and Conclusion

In the previous sections, 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. This is done from a meta-perspective as this fits into the purpose of this article.[66] In the United States, there appears

60 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. Bundeskartellamt, 'Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules' (2 March 2016) <http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2016/02_03_2016_Facebook.html> accessed 27 September 2017. See also, Commission, 'Guidance on the implementation/application of Directive 2005/29/EC' (n 53).

61 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).

62 Commission, 'Guidance on the implementation/application of Directive 2005/29/EC' (n 53) 27.

63 ibid.

64 ibid; art 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.'

65 Van Boom, Garde and Akseli (n 50) 13.

66 We recognise the need for further research on the comparison between the US and EU systems (looking into jurisdictional aspects such as Federal/State vs EU/Member States and analysing relevant jurisprudence) but also on definitions and concepts (such as 'unfair,' 'consumer,' privacy vs competiton, etc).Nor is the purpose of this article to discuss the weakness of US or the European privacy framework as such (hence the reference to complementarity in the title of the article).

***Table 1**. Comparison FTC Act/PCPD*[a]

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.

[a] 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.

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(2), misleading and aggressive practises in Article 5(4) and the prohibited practices on the blacklist. The blacklist particularly illustrates the different legislative approach of both 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 Articles 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 indicative Table 1.

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 E-Privacy Directive (to be replaced by the new E-Privacy Regulation). However, it should be remarked that partly due to lack of competence and experience, actual enforcement 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 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.[67] 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.[68] This should be considered for compliance and enforcement which should, in the first place, be consumer oriented.

From our perspective, a more balanced approach is needed. Cases which mostly concern market behaviour should primarily be solved through market- and consumer-oriented regulation. In this scenario, European market and consumer authorities should play a more active role, whether or not in consultation with data protection authorities based on proper cooperation procedures.[69] It is, after all, their task to speak up for the market and consumer interests.[70,71] Through applying rules on unfair commercial practices, the enforcement of privacy issues could become more effective.[72] However, effective enforcement should not solely rely on the ability to impose fines, but should also focus on prevention and behavioural change. To achieve this, European supervisory authorities could follow the example of the FTC's consent agreements by entering into binding agreements between the authority and a private party. The instrument of 'binding commitments,' very similar to consent agreements, exists as a remedy in regular competition law[73] and improving the effectiveness of binding commitments by introducing further harmonisation is part of a proposal for a new Directive.[74] The existing privacy directive and the GDPR do not mention binding commitments as part of the toolkit for Data Protection Authorities. In our view, harmonising binding commitments as a remedy within

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

68 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 cannot put a price tag on them.

69 In most EU Member States protocols exist for the cooperation between regulators. These are probably a good blue print for national situations where cooperation between data protection authorities and consumer/market regulators is not yet sufficiently covered.

70 Recently the European Commission asked social media companies to comply with EU consumer rules [European Commission, 'The European Commission and Member States consumer authorities ask social media companies to comply with EU consumer rules' (Press release, 17 March 2017) IP/17/631 <http://europa.eu/rapid/press-release_IP-17-631_en.htm> accessed 27 September 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), but also mentions the UCP. This Council Directive is also mentioned in recital 42 of the GDPR. 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' (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).

71 We also see growing interest from competition/consumer regulators and courts in related topics, and although this is not covered by this article we like to give some references: Autorité de la concurrence and Bundeskartellamt, 'Competition Law and Data' (10 May 2016) <http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2)> accessed 27 September 2017, and the announcement of the Italian competition authority to investigate the same issue: Autorità Garante della Concorrenza e del Mercato, '"Big Data": Italian Regulators open a sector inquiry' (Press release, 1 June 2017) <http://www.agcm.it/en/newsroom/press-releases/2384-"dig-data"-italian-regulators-open-a-sector-inquiry.html)> accessed 27 September 2017. We note that in some Member States and on the EU level case law exists or cases are pending based on competition law involving companies dealing with personal data, ie Bundeskartellamt/Facebook: Bundeskartellamt, 'Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules' (2 March 2017); <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html> accessed 27 September 2017; Autorità Garante della Concorrenza e del Mercato, 'WhatsApp fined for 3 million euro for having forced its users to share their personal data with Facebook' (12 May 2017) <http://www.agcm.it/en/newsroom/press-releases/2380-whatsapp-fined-for-3-million-euro-for-having-forced-its-users-to-share-their-personal-data-with-facebook.html> accessed 27 September 2017; European Commission/Google: European Commission, 'Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service' (Press release, 24 June 2017) IP/17/1784 <http://europa.eu/rapid/press-release_IP-17-1784_en.htm> accessed 27 September 2017.

72 On the lack of effectiveness of the European regulatory framework and the reframing of privacy-issues. See also: Bert-Jaap Koops, 'The trouble with European data protection law' (2014) 4 International Data Privacy Law 250–261.

73 art 9 Council Regulation (EC)1/2003.

74 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' (22 March 2017) COM(2017) 142 final.

the GDPR should be seriously considered. In the meantime, and due to the lack of harmonisation, individual EU Member States could include binding commitments in their national regulatory framework as part of the remedies in the context of privacy and data protection.