Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., & Viljoen, S. (2020). The chilling effects of algorithmic profiling: Mapping the issues. Computer Law & Security Review, 36, 105367. https://doi.org/10.1016/j.clsr.2019.105367

This is a postprint version of:

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., & Viljoen, S. (2019). Chilling Effects of Profiling Activities: Mapping the Issues. *Computer Law & Security Review.* https://doi.org/10.1016/j.clsr.2019.105367

The Chilling Effects of Algorithmic Profiling: Mapping the Issues

Authors (in alphabetical order)

Moritz Büchi, *University of Zurich*
Eduard Fosch-Villaronga, *Leiden University*
Christoph Lutz, *BI Norwegian Business School*
Aurelia Tamò-Larrieux, *University of Zurich*
Shruthi Velidi, *BI Norwegian Business School*
Salome Viljoen, *Harvard University*

Keywords: profiling, inferences, chilling effects, surveillance, data protection, privacy, algorithms, big data, digital footprints

Abstract: In this article, we provide an overview of the literature on chilling effects and corporate profiling, while also connecting the two topics. We start by explaining how profiling, in an increasingly data-rich environment, creates substantial power asymmetries between users and platforms (and corporations more broadly). Inferences and the increasingly automated nature of decision-making, both based on user data, are essential aspects of profiling. We then connect chilling effects theory and the relevant empirical findings to corporate profiling. In this article, we first stress the relationship and similarities between profiling and surveillance. Second, we describe chilling effects as a result of state and peer surveillance, specifically. We then show the interrelatedness of corporate and state profiling, and finally spotlight the customization of behavior and behavioral manipulation as particularly significant issues in this discourse. This is complemented with an exploration of the legal foundations of profiling through an analysis of European and US data protection law. We find that while Europe has a clear regulatory framework in place for profiling, the US primarily relies on a patchwork of sector-specific or state laws. Further, there is an attempt to regulate differential impacts of profiling via anti-discrimination statutes, yet few policies focus on combating generalized harms of profiling, such as chilling effects. Finally, we devise four concise propositions to guide future research on the connection between corporate profiling and chilling effects.

(1) Introduction

On January 30, 2019, the Wall Street Journal (WSJ) published an article on how New York life insurers, in the future, may use social media profiles to determine insurance premium rates (Scism, 2019). This prompted the WSJ to issue a series of "life hacks" for insurance surveillance camouflage, including tips on how to behave on social media in order to bypass insurers' profile evaluations. Some of the aforementioned "life hacks" included: (1) do not post photos of yourself smoking, (2) post pictures of yourself exercising (but not while engaging in a risky sport), (3) use fitness tracking devices to show you are concerned about your health, (4) purchase food from healthy online meal-preparation services, and (5) visit the gym with mobile location-tracking enabled (while leaving your phone at home when you go to a bar). As much as these recommendations impose on and restrict daily life, they may seem relatively benign. When taken together, such modifications of social media and mobile phone usage can have a considerable impact on human development, namely via autonomy, creativity, social identity experimentation (without fear of repercussions), and multifaceted deviance from dominant sociocultural norms. This modification of behavior prompts the question of whether these practices, and the regulatory conditions under which they operate, deter individuals from legitimate behavior, i.e., whether they create chilling effects.

In this article, we address the following question: Do profiling activities, conducted by corporations, lead to chilling effects? Although a seemingly simple question, chilling effects are neither apparent and straightforward nor always directly and exclusively linked to the consequences of profiling. More often than not, chilling effects can be intangible and difficult to identify and quantify (Cas et al., 2015). While analyzing behavioral changesis of general interest, we focus our attention on behavioral *deterrence* or inhibitions, or so-called chilling effects, of profiling activities. Therefore, we make a distinction between behavior that aims to *avoid* an undesired image or action (e.g., chilling effects), and other forms of behavioral changes, which aim to *approach* a desired image or action (e.g., assertive self-presentation) (Marder et al., 2016; Schütz, 1998). In this sense, we rely on Penney's (2017) definition of chilling effects, used in the context of state surveillance, as well as on Marder et al.'s (2016) broader definition, which understands chilling effects as the "impact of surveillance by the audience(s) on constraining behavior" (p. 582). These behavioral constraints can manifest as self-censorship, self-restraint, or as silencing effects. We understand profiling, in this context, to broadly include any technique that automatically processes data

related to individuals in order to develop predictive knowledge for the purpose of constructing profiles, forming a basis for future decision-making (Bosco, Creemers, Ferraris, Guagnin, & Koops, 2015; Hildebrandt, 2008; see definition in Section (2) What is Profiling?).

We first explore how corporations use profiling techniques to translate data points into inferences in Section (2). By defining the term profiling and elaborating on the resulting new knowledge produced - and used - by corporations in the digital age, we lay a foundation to discuss the impacts of profiling in Section (3). Next, we define chilling effects to help analyze the link between profiling algorithms and state surveillance by government authorities. In this section, we start by taking a broader lens by first determining the effects of corporate profiling, via a comparison to state profiling. Then, we survey the limited body of literature on corporate surveillance techniques via profiling and its impact on society and individuals. In Section (4), the article transitions to the regulatory frameworks currently in place that might address corporate profiling. We contrast the European approach, which focuses on data protection law and the central role of the GDPR, with the US approach, which comprises of sector-specific consumer protection and anti-discrimination laws. Finally, we derive a roadmap for future interdisciplinary work and for empirical assessments that can further explore the relationship between chilling effects and corporate profiling in Section (5), comprising of five focus areas for research. Section (6) offers a brief concluding discussion and summary.

(2) Profiling: From Data Points to Inferences

What is Profiling?

Both the public and private sectors are interested in building reliable inferences that can guide their decision-making. While we include literature on profiling activities by government authorities and the link between profiling and state surveillance, the main focus of our article is how corporations utilize algorithmic profiling and the effects this may have on the profiled individual. Profiling is defined here as the systematic and purposeful recording and classification of data related to individuals—a profile is thus a compilation of data referring to an individual. Moving into the digital age has transformed profiling into automated algorithmic profiling and—in the age of big data—has enabled the creation of profiles from much more extensive data sources. Some of the core drivers of this development are the increase of digital data

availability, a shift from demographic to individualized targeting, real-time experimentation, and platformization (Tufekci, 2014).

Automated profiling is a result of the data mining process (Hildebrandt, 2008). In this process, algorithms mine for patterns of correlations within the data. Thus, profiling is inductive: it produces new knowledge from existing knowledge by analyzing correlations (Bosco et al., 2015). Although correlations only contain information on whether the pattern of deviance from a mean is similar for two variables of interest, this still holds predictive potential: without any reference to a cause, we can estimate "a probability that things will turn out the same in the future" (Hildebrandt, 2008, p. 18). In this way, profiling algorithms embody a discovery-based approach more so than a traditional assumption-driven approach (Hildebrandt, 2008 referring to Custers, 2004; Bosco et al., 2015; EU FRA, 2018). This reflects a more general distinction between the social science and computer science approaches to data analysis (see Wallach, 2018): a parsimonious, interpretable, and thus, transparent explanatory model to guide or inform human reasoning, typical for the former, is qualitatively very different from a complex, non-interpretable predictive model ("black box") geared towards replacing human reasoning, which is typical for the latter. On the relevance of this discovery-based approach, which we propose is the dominant one among corporate profiling activities, Wallach (2018) notes that "[t]here is a substantial difference between a model that is 95% accurate because of noise and one that is 95% accurate because it performs perfectly for white men, but achieves only 50% accuracy when making predictions about women and minorities" (p. 44).

The private sector is, in particular, interested in the classification of data points that relate to a specific user (or category of users). Examples include data relating to online and offline purchases, census records, online surfing behaviors and interests, location data, and the like. Such data are valuable as they allow for the creation of profiles that enable a service provider to target individuals through ads or product/service placement. Described as a panoptic sort in the 1990s, there are many examples that illustrate how an individual's information can be used to determine their economic value (Gandy, 1996). One prominent example is Facebook's "Lookalike Audiences" service for advertisers, which matches the demographic and interest-based profiles of existing users and customers to prospective ones. This enables scaled targeting, even with regards to race - a discriminatory user attribute that is not directly available by itself (see Speicher et al., 2018). Another example of how the private sector creates profiles of users. Twenty mobile applications, which researchers had flagged as highly "in-

trusive" in terms of data gathering, were analyzed. By illustrating the location patterns of one individual in an interview setting, the interviewee became aware of the amount of data collected New York Times (2018). She acknowledged that her increased awareness over the created location profiles made her feel uncomfortable. The question of whether such profiles might chill someone's behavior was left unanswered.

From Profiles to Inferences

"Successful pricing strategies, marketing campaigns, and political campaigns depend on the ability to optimally target consumers and voters." (Chen, Fraiberger, Moakler, & Provost, 2017, p. 197). Therefore, corporations have an incentive to profile users through the exploitation of commercially derived inferences. Corporations primarily create profiles to more effectively position relevant, targeted ads to their potential customers. Advertising may be a legitimate business, yet this carries great potential for malicious uses of the data if the corporation's interests shift, or third parties, including governments, gain access to these profiles (see Christl, 2017).

Profiles are often fed with personal data provided by the users themselves, but the automated inferences drawn from existing, "non-sensitive," or voluntarily disclosed information can stray substantially from any human judgment or possible inferences imagined by the user who provided their data. Corporations can build profiles based on different data types. Rao, Schaub, and Sadeh (2015) looked into profiles from three different companies—Bluekai, Google, and Yahoo—and listed the following data types that were recorded: demographic data (e.g., sex, age, education, income range, home value), data on interests and attitudes (e.g., health-related searches, likely travel destinations, likelihood of buying American), behavioral data (e.g., past purchases), geographic location, technical specifications (e.g., IP address, browser), and predictive data (e.g., credit card interest score). Consequently, inferences about individuals or groups are made based on profiling. Inferences encompass predictions about future actions or inactions, general characteristics, and specific preferences. These data categories can paint a detailed picture of an individual by combining "banal" information, such as the browser version used, with predicted attributes, such as home value. Inferences can be communicated overtly to the user (e.g., recommendations for a specific music show or restaurant), can be merely assumed by the user (e.g., advertisement that is not obviously related to a past search), or can be hidden entirely (e.g., data being assembled and sold by data brokers, such as Acxiom, or by other third parties, as was the case in the Cambridge Analytica scandal). Users certainly express concerns about how their data is used, yet counter measures offered by corporations, such as

anonymization, constitute a poor corrective because of the possibility to re-identify or deanonymize profiles through the combination of data sources (Chen et al., 2017).

What harms may users experience from such use of their data? While being shown relevant ads could be perceived as beneficial, discrimination is one example of a negative outcome (Noble, 2018). What we focus on here, however, is the more subtle and long-term effects of corporate profiling activities, and/or users' fragmented awareness thereof, resulting in a potential deterrence from unhampered online behavior. This may be in the form of unrestricted information seeking, self-expressing on social media, or even just selecting entertaining content. How does the latent awareness of algorithmic profiling affect behavior?

(3) Chilling Effects of Profiling Activities

The Link between Profiling and Surveillance

To understand the consequences of profiling, we first draw a link between profiling and surveillance. Relying on Lyon's definition, we know surveillance to mean the collection and processing of personal data for control or influence (Lyon, 2001). A particular form of surveillance, known as dataveillance, refers to the continuous monitoring of citizens on the basis of their meta data or more broadly, their online data (Raley, 2013; Van Dijck, 2014). Unlike traditional surveillance, which aims to monitor for the purpose of gathering details for a specific, given purpose (Lyon, 2014), dataveillance allows for the constant and continuous tracking of data for "unstated preset purposes" (van Dijck, 2014, p. 205). This form of surveillance allows not only for the mass collection of personal data, but also for the ability to constantly build and refine profiles related to individuals and their behaviors. These profiles can then be utilized to develop inferences on future behavior and to predict decision making (Schermer, 2011).

In the private sector, the competitive advantage of the datification of people's intimate and social lives, in the era of big data, has caused an increase in the capabilities and advancement of dataveillance techniques (Sax, 2016; Van Dijck, 2014). Moreover, routine surveillance of our daily transactions and social interactions has become easier to collect and cheaper to store (Gandy, 2006). This further incentivizes corporate actors to maintain large databases of records of our behaviors that can be algorithmically aggregated into profiles, which can be searched at any point in the future (Lessig,

1999; Gandy, 2012). In this article, we focus on how the prevalence of dataveillance techniques is leveraged to conduct profiling activities in the private sector.

In the following sections, we connect the surveillance discourse to chilling effects. We start by discussing the literature on state surveillance and chilling effects. This lays the foundation for the subsequent portions on the profiling practices of corporations and the resulting chilling effects. The focus of this work, algorithmic profiling conducted by corporations, is part of a more extensive "system of surveillants and surveilled" in digital societies (*see* Figure 1) that helps to inform this under-researched angle on chilling effects.

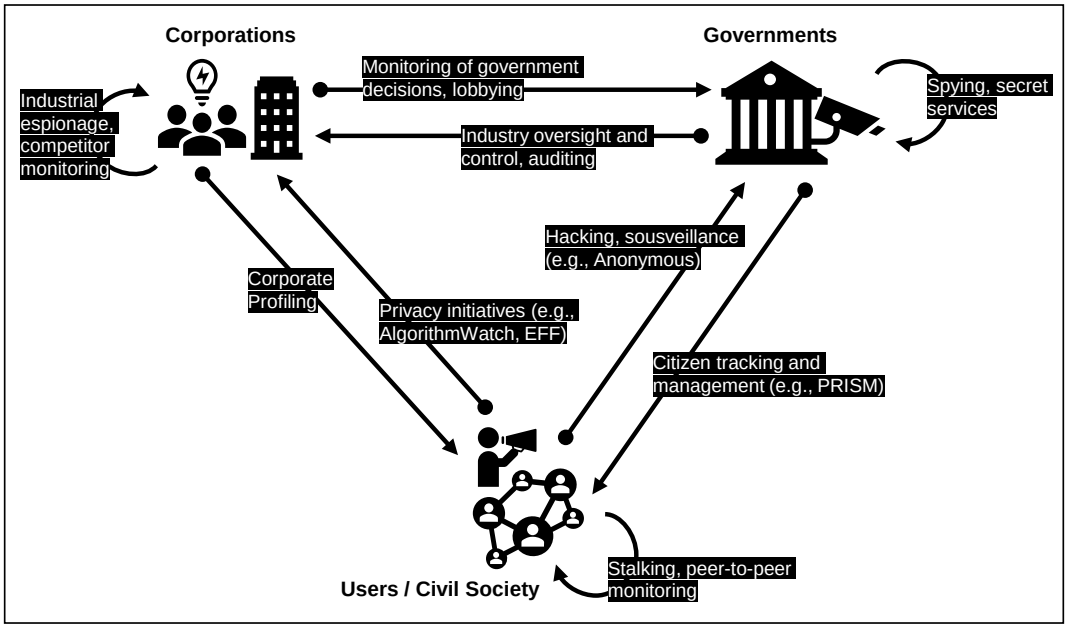

Figure 1. System of surveillants and surveilled in digital societies.

Chilling Effects of State Profiling Activities

With the emergence of online government surveillance, there has been much interest in understanding how state surveillance leads to both behavioral modifications and chilling effects. The leading theory on chilling effects was initially proposed by Schauer (1978), who defines chilling effects as an "act of deterrence" or as the "fear, risk, and uncertainty" in regulations that may "deter people from exercising their rights" (p. 689). Until recently, the debate about online chilling effects was largely conceptual and legal, with limited empirical evidence on how online state surveillance deters people from participating freely on the Internet (Penney, 2017). In fact, and

despite ample adjacent literature (see below on the spiral-of-silence and privacy paradox), we found very few empirical studies linking state dataveillance explicitly to behavioral modifications and chilling effects. The relative recency of the revelations on the extent of state dataveillance and the difficulty of empirically isolating chilling effects might account for this scarcity of neither conceptual nor legal research. Penney's (2017) study on Wikipedia activity after the NSA/PRISM surveillance revelations of June 2013 served as the first empirical analysis of online chilling effects. He distinguished four types of online chilling effects: 1) from a statute or regulation with a penalty that prohibits a certain online activity (Schauer, 1978); 2) from state or non-state data surveillance (Solove, 2006, 2007)[1]; 3) from vague laws in the legal process with a personalized threat of penalty (Renas, Hartmann, & Walker, 1989; Barendt et al., 1997); and 4) "secondary chilling effects", where others in a user's social network (not the users themselves) are chilled. These results illustrate that government surveillance online – in this case, by the NSA after the Snowden revelations – tends to chill people's online activities (Penney, 2017). Interestingly, this finding contradicts existing literature on the "privacy paradox" phenomenon, which states that discrepancies exist between a user's concern for privacy and their actual behavior taken to protect their data (Barth & De Jong, 2017). Penney (2017) challenges this theory by claiming that users are reflecting their privacy concerns in their online behavior by not engaging in certain online activities due to privacy concerns about surveillance.[2]

---

[1] Note that Penney's findings are consistent with Solove's approach, which discusses how these chilling effects are indicative of a broader "surveillance related pollution" – the larger self-censorship and conformity that is a result of mass surveillance (Solove, 2006; Penney, 2017).

[2] The rich literature on the privacy paradox is summarized in two systematic literature reviews (Barth & De Jong, 2017; Kokolakis, 2017) and one meta-analysis (Baruh, Secinti, & Cemalcilar, 2017). These summaries mostly corroborate Penney's (2017) point, as they show the absence of a privacy paradox on aggregate across most contexts, except social network sites (Baruh et al., 2017). Moreover, they suggest a temporal trajectory, where older studies find a privacy paradox but newer studies often fail to do so (Kokolakis, 2017), indicating an awareness change and learning effect over time.

Other recent studies have corroborated Penney's account of online chilling effects due to state surveillance. Marthews and Tucker (2017) discovered a chilling effect on users' Google search behavior after the June 2013 NSA/PRISM surveillance revelations. They looked at whether search traffic for privacy-sensitive terms reduced after these revelations. Their results provided empirical evidence of how surveillance revelations can cause a significant chilling effect on a user's willingness to search certain terms online. Both Penney's and Marthews and Tucker's studies are primarily based on natural experiments. However, adjacent survey-based research has looked into self-censorship across contexts and the factors which influence it. For example, Hampton et al.'s (2014) study on the public perception of the Snowden revelations in the US showed that 86% of Americans were willing to discuss this topic in person, but only 42% of Facebook and Twitter users were ready to post about it online. The authors interpret the findings within the spiral-of-silence theory (see below). While Hampton et al. (2014) did not control for concerns about government dataveillance in their survey, the sizable difference in willingness to discuss the topic in person and on social media suggests that the context of disclosure matters (Nissenbaum, 2004). It seems plausible that the affordances of the social media environment, including persistence and searchability (boyd, 2010), were seen as detrimental for discussing this topic uninhibitedly. Manohka (2018) connects Hampton et al.'s (2014) study to research on chilling effects and the Snowden revelations more broadly, using a Foucauldian lens.

"Indeed, even if a message posted on social media, or an Internet search query, or a purchase made online, or a petition signed, does not trigger an immediate reaction (e.g., from security services or from social media 'friends'), it might always do so at some future point in time because the information about it is stored in some database and may, for one reason or another, be found and retrieved by some actor. And, as the available studies on the 'chilling effect' examined earlier have demonstrated, the awareness of this on the part of the 'watched' is increasingly present." (Manokha, 2018, p. 232)

Finally, Stoycheff, Liu, Xu and Wibowo (2018) examined how the perception of being surveilled by the government affects how individuals carry out sensitive online activities. Their results "point to a restrictive—but not absolute—chilling effect that persists across different online populations, experimental stimuli, and political contexts" (p. 603). Using two experiments in the US and contextualizing the data analysis within a Panopticon lens, the authors demonstrated state surveillance-driven chilling effects on not only illegal behavior, but also on potentially desirable political behavior.

From State to Corporate Profiling Activities

While traditional forms of state surveillance included techniques such as phone-tapping or photography (Agre, 1994), contemporary methods of (mass or bulk) surveillance can gain insight into our personal lives by accessing how we shop, manage finances, take care of our health, apply for jobs, and maintain social relationships (Bernal, 2016).

In today's data economy, surveillance by the state works in conjunction with commercial partners. Bruce Schneier (2013) described what is known as the "private/public surveillance partnership" – a concept used to illustrate the cooperative effort undertaken between the government and corporations to collect mass amounts of personal data from users. He explains how our constant interactions with computers and networks produce a large amount of data, data that is collected by corporations. This type of data can be intentionally given by the user – either via Google, Facebook, or any other free service – or inadvertently given through our regular use of our phones and credit cards (Micheli, Lutz, & Büchi, 2018). In turn, the state can collect data from these corporations, rather from the users directly, creating a "surveillance partnership" between the state and private corporations.

This surveillance partnership only exists because corporations have strong motivations to collect mass amounts of personal data from users. With unprecedented access to user data, corporations can conduct a variety of activities to better understand and predict customer behavior. A New York Times investigation stated that the location-targeted advertising market, based on location data from different smartphone apps, reached $21B in 2018 (Valentino-DeVries, Singer, Keller, & Krolik, 2018). Companies can choose to use or analyze this data either for their purposes or sell this data to advertisers, retailers, or even hedge funds—all to reveal patterns and to "seek insights into consumer behavior" (Valentino-DeVries et al., 2018). A spokesperson from GroundTruth, a location technology company, explains how tracking can be used to reveal a person's preferences (Valentino-DeVries et al. 2018). GroundTruth claims they can not only determine who a person is but can also predict and influence what a person will do next, simply based on where these users have been or are going. This information is a type of inference that can then be used by companies to create profiles of its customers.

For example, Google paid MasterCard millions of dollars for its ability to track if Google's online ads led to purchases in physical stores (Bergen & Surane, 2018).

Google's program, known as "Store Sales Measurement," claims to have access to "approximately 70 percent of U.S. credit and debit cards through partners" without gathering personally identifiable information. Google can then "anonymously match these existing user profiles" to purchases made in the physical stores (Bergen & Surane, 2018). Another example is FriendlyScore, a UK-based startup whose business model focuses on harnessing social media data to create a credit "scorecard" that is then sold to credit lenders. This "scorecard" compiles all publicly available online information, including wall posts, check-ins, and requested deliveries. These profiles are then used as risk assessments that aim to "predict the future intentions" of borrowers, determining whether or not a financial institution should provide a loan to a user (Holloman, 2014).

Two crucial issues become evident in these examples. First, once digital data is created, typically about a single type of information such as location, it can be used in other contexts and converted, through inferencing, into other types of information (e.g., preferences). Second, combining data from different sources is commonplace and matching across platforms is routinely done.

Chilling Effects as a Result of Peer Surveillance

Literature on Chilling Effects of Social Platforms

Existing literature on chilling effects has provided evidence of different behavioral modifications, both online, through self-censorship and behavior customization, as well as offline via impression management (Marder et al., 2016). However, the literature tends to conceptualize chilling effects primarily as a response to peer monitoring or government monitoring; we are not aware of in-depth studies on the chilling effects of corporate or public/private partnership monitoring and profiling. We thus proceed to discuss relevant adjacent studies that are informed by theories in media and communication.

The "spiral of silence" (SoS) theory, which originated in communication and public opinion research (Noelle-Neumann, 1974), illustrates how individuals monitor their social environments and develop perceptions about which opinions are popular (i.e., the majority) and which ones are less popular (i.e., the minority). SoS refers to the process of self-censorship that occurs when an individual believes their opinion belongs to the minority opinion, resulting in a stronger dominance of the majority opin-

ion over time. In the age of social media and especially after the 2013 Snowden revelations, SoS saw a revival. Stoycheff (2016) observed a decrease in a willingness to speak out on a variety of online platforms, such as online forums (Kim, Kim, & Oh, 2014; Yun & Park, 2011) and social networking sites (Fox and Warber, 2015), in relation to a person's perceived climate of opinions. Stoycheff (2016) was also responsible for connecting the chilling effects theory with SoS theory by providing empirical evidence that, under certain conditions, knowledge about government surveillance may threaten the willingness to speak out on minority opinions, contributing to the reinforcement of majority views. Moreover, in an attempt to conform to the majority, she observed that users displayed both a silencing as well as a self-censoring effect (Stoycheff et al., 2018).

Literature on Chilling Effects of Social Pressures

In addition to chilling effects that result from government surveillance, other research has documented evidence of chilling effects due to social pressures or peer surveillance. Manokha (2018) argued that online self-censorship and self-restraint were primarily due to large audiences of peers, as opposed to state or corporate surveillance concerns. Similarly, Brandtzæg, Lüders, and Skjetne (2010) found that conformity on social media sites occurs when individuals are exposed to increased surveillance by other members online. Marder et al. (2016) provided corroborating evidence of how "peer to peer monitoring" (Andrejevic, 2004) can result in chilling effects, even in the offline world. When users are aware of online audiences in the offline world (e.g., attending a party with some of your Facebook friends), they tend to modify or censor their behavior in the offline domain in anticipation of the online consequences (Marder et al., 2016). Das and Kramer (2013), in a large-scale study based on behavioral data from 3.9 million Facebook users, found that 71% percent of these Facebook users had engaged in "last-minute self-censorship" within a 17 day period. These users had already formulated a post or comment, but then decided to delete it before posting. Demographic characteristics, audience control characteristics (e.g., how strict someone's privacy settings are and whether the post was supposed to occur in a group), and network composition (e.g., political opinion heterogeneity of someone's Facebook friends) were key factors in explaining this last-minute self-censorship.

These findings on chilling effects from (the fear of) peer monitoring can be explained by the context collapse theory (Marwick & boyd, 2011). On more established social media platforms, such as Facebook and Twitter, users especially face the challenge of

multiple audiences with different interests. In other words, on such platforms, different contexts come together and collapse, which can lead to self-presentation strategies that appeal to the "lowest common denominator" (Hogan, 2010). Ultimately, this may lead to an uncritical public sphere: individuals only post inoffensive and newsworthy content (such as job updates, graduations, family news, or funny videos) that most of their friends or followers might be interested in, refraining from posting more controversial or politically charged content. Thus, in many online environments - particularly on social media - state, corporate, and peer surveillance coexist, leading to a distinction between social privacy and institutional privacy (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). This makes it difficult to isolate the chilling effects of specific types of surveillance.

Other Behavioral Effects due to Profiling Activities

Chilling effects are not always apparent, straightforward, or directly linked to the consequences of profiling. They are frequently intangible and difficult to identify or quantify (Cas et al., 2015), resulting in limited research on the correlation between profiling and chilling effects. However, scholars have discovered other forms of behavioral effects, such as the customization of behavior and behavioral manipulation, that can result from profiling.

Customization of Behavior

Schermer (2011) claimed that a fear of the government's extensive profiling capabilities could reduce a user's willingness to speak out and can limit a user's participation in public discourse. Schermer (2011) also argued that this fear, and its respective behavioral consequences, can materialize whether or not the profiling itself is effective. However, the effectiveness of profiling remains under-researched and is difficult to assess given the confidential nature of profiling algorithms and black-boxing due to the complexity of self-learning mechanisms (Burrell, 2016; Pasquale, 2015). Other authors suggest that individuals customize their behavior in anticipation of the perceived expectations of the profilers (Gräf, 2017; Koops, 2008). Dumortier (2010) argues that behavior customization, as a result of profiling, can risk individual autonomy (Kandias, Mitrou, Stavrou, & Gritzalis 2016).

Behavioral Manipulation

Since a majority of users are unaware of how profiling activities can impact our preferences, actions, and beliefs (Gräf, 2017; Hildebrandt, 2008), discoveries of how Facebook allows advertisers to target vulnerable teenagers (Machokovech, 2017) or of how Uber influences the behavior of customers and drivers (Calo & Rosenblat, 2017) have become of interest to the broader population.

Manipulation is best described as a hidden influence or the "covert subversion of another person's decision-making power" (Susser, Roessler, & Nissenbaum, 2018, p. 2). In contrast to persuasion, which occurs in plain sight, manipulation occurs without knowledge of the forces at play (Susser et al., 2018; cf. also Zarsky, 2018). Unlike coercion, manipulation exploits the manipulee's (cognitive or affective) weaknesses (Susser et al., 2018). In other words, manipulation, in the digital world, not only has a technical component - namely the ability to tailor content to individuals, based on collected data traces, through the use of advanced data analytics tools - but also a psychological one through the exploitation of psychological vulnerabilities (Zarsky, 2018). Automated manipulation exploits human weaknesses and behavioral biases (for an extensive overview of behavioral research and market manipulation (see Hanson & Kysar, 1999). Thus, even if Gräf (2017) argues that "we cannot take profiling into account when planning future actions, even when we know it somehow impacts our options" (p. 4), literature on behavioral biases will tell us that even if we knew how profiles are used, we would likely still be subject to automated manipulation.

The literature argues that information technology has made manipulation considerably easier and has enlarged the scope of manipulation practices (Susser et al., 2018; Zarsky, 2018). First, because of the widespread use of profiling algorithms (or surveillance tools); second, because digital platforms and the sharing economy encourage dynamic, interactive, and constant exchange - creating personalized architectures; third, because we leave data traces in almost all aspects of our lives (i.e., so much that we do generates data and can be aggregated to a whole) (see Susser et al., 2018; Zarsky, 2018).

It is outside the scope of this paper to extensively elaborate on why manipulation is problematic. While we intuitively consider manipulation "wrong", automated manipulation is primarily harmful because it undermines an individual's autonomy (Susser et al., 2018; Zarsky, 2018). Autonomy constitutes the ability to choose between reasonable options and to make an informed decision concerning one's own life (Dworkin, 1988). Corporations can manipulate not only an individual's economic

choices and preferences - which can lead to inefficient market outcomes (Zarksy, 2018) - but also have the capacity to shape social and political behaviors, posing a threat to democratic and free societies.[3]

Gaps in the Literature: Chilling Effects of Corporate Profiling Activities

Despite an increasing interest in data-based surveillance, in general, and chilling effects in particular, empirical research is scarce and scattered. The few studies that have attempted to empirically assess chilling effects have primarily focused on government (or state) surveillance (e.g., Penney, 2017), not on corporate surveillance practices. The identification and isolation of corporate chilling effects might prove challenging due to the Gordian knot of corporate surveillance, government surveillance, and peer monitoring in many online contexts. Therefore, the intricacies of how corporate profiling practices constrain individuals' behavior remain under-researched and under-developed.

(4) Regulating Profiling Activities of Corporations

While neither European nor US legal regimes explicitly regulate corporate chilling effects, the chilling capacity of data-based corporate surveillance, discussed in Section 3, should be of central concern to legal scholars and practitioners interested in understanding and responding to the harms that may result from corporate surveillance activities, as well as those who are concerned more traditionally with chilling effects that result from government surveillance.

The section below reviews how legal regimes in both the EU and the US may interact with corporate chilling effects. It also attempts to provide an overview of the gaps

---

[3] Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes. Council of Europe. https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168092dd4b

that exist in both regimes, as well as identify areas where the law may have the capacity to address certain kinds of chilling effects.

European Approach

Data Protection Law

In 2011, the Special Eurobarometer on attitudes towards data protection and electronic identity in the European Union revealed that many Europeans feel uncomfortable with practices involving online profiling (Special Eurobarometer, 359). It is, therefore, not surprising that the General Data Protection Regulation (GDPR), which was established to promote trust in the digital economy, includes a definition of profiling (cf. Rec. 7 GDPR). A Working Party 29 (WP29) advice paper, adopted in May 2013, had also urged policymakers to include a definition of profiling in the GDPR.[4] In line with its earlier Opinion 01/2012 (WP 191), the WP29 reasoned that the creation of profiles could significantly impact an individual's right to data protection and therefore, aside from defining the term, more should be done to explain the risks of profiling.

These concerns encouraged policymakers and data protection authorities to examine the issue more closely. Nowadays, case law from the Court of Justice of the European Union (CJEU) and the GDPR both emphasize the importance of providing individuals with safeguards against undesirable corporate profiling activities (Petkova & Boehm, 2018). The GDPR defines automated profiling as: "any form of *automated processing of personal data* consisting of the use of personal data *to evaluate certain personal aspects* relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health,

[4] See Article 29 Data Protection Working Party, Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, Adopted on 13 May 2013, available at: <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf> (last visited March 6, 2019).

personal preferences, interests, reliability, behaviour, location, or movements" (Art. 4(4); emphasis added).[5]

Profiling is thus composed of three elements: 1) the automated processing of 2) personal data, with the objective to 3) evaluate particular aspects of a specific natural person. While the first two elements are critical terminologies known (or at least, often debated and substantiated in case law) within the European data protection framework, the third element, namely the evaluation of personal aspects, has been less well-defined.

According to the WP29 and its "Guidelines on Automated individual decision-making and Profiling" which was last revised and adopted in February 2018, the "use of the word 'evaluating' suggests that profiling involves some form of assessment of judgment about a person" (WP29, Opinion WP251rev.01, p. 7). If, from the classification of data, no such assessment of judgment results, e.g., because it is an analysis for merely statistical purposes or for acquiring only an aggregated overview, then it does not fall under the concept of profiling (WP29, Opinion WP251rev.01, p. 7). However, if the gathered data is evaluated to determine the characteristics of an individual or a specific group of individuals, especially to predict an individual's or group of individuals' behavioral patterns, interests, or abilities; then such processing falls under the scope of the GDPR's profiling definition (WP29, Opinion WP251rev.01, p. 7). A typical example of such profiling activities are those conducted by data brokers who collect data from different private and public sources and develop profiles. These profiles are then sold to companies to better target goods and services to those individuals or groups (Symons & Bass, 2017). As Symons and Bass (2017, p. 19) explain, certain

[5] Even though the Council of Europe Recommendation CM/Rec (2010)13 (Council of Europe 23 November 2010) inspired the definition of profiling within the GDPR, the Regulation did not adopt the Council's definition of profiling. The Council defines profiling as any "automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes". See Council of Europe Recommendation CM/Rec (2010)13 (Council of Europe 23 November 2010), available at <https://rm.coe.int/16807096c3> (last visited March 6, 2019).

companies "can combine data from multiple sources to build a personal profile of more than 1,000 pieces of information (...) from this, they can derive an even larger number of behavioral insights, primarily about an individual's buying intention across a range of different products."

A particular focus of the GDPR is automated decision-making. Profiling is seen as a means to enable automated decision-making and is thus typically included within the term. Profiling can sometimes also involve human decision-makers. In this sense, the profiling process contains the following elements: the collection of data, the development of the model by either humans or (machine-learning) algorithms, and finally the decision-making itself (Kamarinou, Millard, & Singh, 2017).

A data subject has the right to demand not to be subject to such automated decision-making (which includes profiling), if such a decision produces legal effects or similarly significant effects (Art. 22(1) of the GDPR). According to the WP29, even if the decision-making is not "purely automated" because the data controller has "fabricated" some human involvement within the decision-making procedure (e.g., a human-in-the-loop who merely applies the profiles to individuals or groups of individuals without any actual influence on the result), the data controller will remain subject to the obligation of Art. 22(1) of the GDPR (WP29, Opinion 2018, WP251 rev 01, p. 21). Furthermore, "the GDPR does not just focus on the decisions made as a result of automated processing or profiling (...) but it (also) applies to the collection of data for the creation of profiles, as well as the application of those profiles to individuals" (WP29, Opinion 2018, WP251 rev 01, p. 6).

It is important to note that the above-cited opinions and guidelines of the WP29 are by no means legally binding and that the literature has criticized the legal shortfalls of the European data protection law when it comes to regulating profiling activities and inferential analytics (Wachter, 2019; Wachter & Mittelstadt, 2018). One major criticism is that the focus of data protection law rests too much on the processing of "personal data" (i.e., the "input" into a processing system) and offers merely procedural rights, rather than focusing on the "output" that results from inferential analytics or on regulating the impact of automated decision-making. In fact, Wachter and Mittelstadt (2019) thoroughly analyzed the applicability of the GDPR on inferential analytics. They noted that the WP29 remained silent on how the GDPR classifies the processes that lead to inferences; moreover, the jurisprudence of the CJEU, so far, applies data protection law only to input data and does not ensure the transparency and accuracy of decision-making processes. This lack of regulation might be problematic

with respect to the private sector's use of profiles and inferential analytics, as they do not have to adhere to predefined, and through democratic means, legitimized decision-making standards (Wachter & Mittelstadt, 2018).

Similarly, another criticism highlights that the regulatory framework, which addresses corporate profiling activities, firmly focuses on the collection and processing of personal data; however, this neglects scenarios in which companies do not need to rely on personal data to create traceable profiles of individuals. In fact, Gräf (2017), notes that companies can make inferences about individuals without requiring the processing of personal data or without the need to identify them. Due to privacy law restrictions, for example, online marketers increasingly base their profiling algorithms on statistical inferences derived from the available information because specific, personal, characteristics are hard to access or observe directly (Chen et al., 2017). In such a setting, the GDPR could be bypassed altogether because identification (or possible identification) is no longer necessary for profiling (Gräf, 2017; George, Reutimann, & Tamò-Larrieux, 2018). If non-identifiable individuals are adversely influenced and affected by profiling activities, then they need to look for other (legal) remedies to address these challenges, such as non-discrimination law (Schreurs et al., 2008; Schermer, 2011; Le Métayer and Le Clainche, 2012; Custers et al., 2013; Mantelero, 2014; Taylor, 2017; EU FRA 2018).

Beyond the GDPR: Declaration aiming to reduce potential algorithmic-inferential discrimination

While the GDPR tries to address the consequences of profiling with personal data, its recitals (in particular 75 and 85) indicate that policymakers were aware of the discriminatory potential of algorithmic inferences and decision-making as well as the associated risks for the fundamental rights and freedoms of natural persons. It is questionable whether the GDPR is the right instrument to address the discriminatory consequences of the processing of personal data.

According to the Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, data protection laws do not suffice in protecting against discrimination. Humans have the right to form opinions and make decisions independently of automated systems that emanate from advanced digital technologies (Council of Europe, 2019). The Council of Europe (2019) has expressed concerns regarding the consequences of the growing capacities of machine learning tools, including choice prediction, the influence of emotion and thought, and the ability to alter,

sometimes subliminally, an anticipated course of action. The Committee of Ministers agreed on the central problem underlying these advancements: the power they confer to those using and developing fine-grained, subconscious, and personalized-level-of-persuasion algorithmic tools, especially in situations where oversight and control are conspicuously absent. This type of power is alarming because it "may have significant effects on the autonomy of individuals and their right to form opinions and take independent decisions" (Council of Europe, 2019), going against the foundational belief that the dignity of humans lies on being independent moral agents.

In this respect, the Council of Europe (2019) appraises that inferences about intimate and detailed information from individuals do affect the exercise of human rights in a much broader sense than the mere notion of personal data protection and privacy. In their words, this process "supports the sorting of individuals into categories, thereby reinforcing different forms of social, cultural, religious, legal and economic segregation and discrimination."[6] Indeed, data-driven technologies prioritize certain values over others, shaping the contexts and environments in which individuals (users and non-users) process information and make decisions. In a way, these technologies are discriminatory by nature, challenging and blurring the negative impacts of such discrimination.

---

[6] In Europe, non-discrimination is enshrined in Art. 21 and 23 of the European Charter of Fundamental Rights (EU CFR) prohibits any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.# This right has been spelled out in several directives, including the Directive 2000/43/EC against discrimination on grounds of race and ethnic origin, the Directive 2000/43/EC against discrimination on grounds of race and ethnic origin, the Directive 2000/78/EC against discrimination at work on grounds of religion or belief, disability, age or sexual orientation, Directive 2006/54/EC equal treatment for men and women in matters of employment and occupation, the Directive 2004/113/EC equal treatment for men and women in the access to and supply of goods and services and the Directive Proposal (COM(2008)462) against discrimination based on age, disability, sexual orientation and religion or belief beyond the workplace.

United States Approach

Privacy Laws

Unlike the EU, the US does not directly regulate corporate profiling activities and lacks comprehensive legislation governing data protection. The general rule in the US is that non-governmental profiling activities are subject only to the contractual terms of data collection and use, agreed to by the user and the corporation, at the point of collection. Instead of being subject to direct regulation, the regulation of corporate profiling activity in the US takes the form of regulatory regimes that attempt to place restrictions 1) on the scope and terms of collection and use of user data; or 2) on the scope and terms of the decisions that can be made about people based on corporate profiling. The first approach encompasses traditional, sector-specific US privacy law and consumer protection regimes. The second approach is primarily achieved via anti-discrimination laws.

First, restrictions on the collection and use of profiling data are regulated by privacy and consumer protection laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[7] Title II of HIPAA establishes procedures for maintaining the privacy and security of individually identifiable health information and creates civil and criminal penalties for violations. While some scholars argue that profiling activities should fall under HIPPA due to the sensitivity of the data collected by platforms (Stark, 2018), other experts find HIPPA to be inadequate with regards to profiling activities. The latter argue that it does not cover health data shared by online shopping services (e.g., if a person buys a knee brace), health data collected by tech companies (e.g., Fitbit, Apple Watch), or any of the digital traces left online - all of which could provide insights into an individual's health (Chen, 2019; Reece & Dandforth, 2017).

[7] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936.

Another regulation that might cover profiling activities is the Fair Credit Reporting Act (FCRA), which includes activities conducted by consumer reporting agencies, users of consumer reports, and furnishers of consumer information.[8] FCRA has been used in the past to curb certain profiling activities. In 2001, for instance, the US Court of Appeals for the District of Columbia upheld the FTC's decision to order TransUnion Corp. to stop selling consumer reports, in the form of targeted marketing lists, under FCRA.[9] Scholars have argued that FCRA may apply to the use of social media profiles to determine eligibility for employment (Fair, 2011) and Facebook's system of rating and profiling users' trustworthiness to sell to third parties (Levitin, 2018). Lastly, the Children's Online Privacy Protection Act of 1998 (COPPA) protects against the online collection of personal information of children under 13 years of age and of children with disabilities.[10] With respect to the limits on corporate profiling, COPPA imposes specific affirmative responsibilities on operators to protect children's privacy and safety online, including restrictions on marketing to those under 13.

Meaningfully regulating corporate profiling activities in the US via HIPAA, FRCA, and COPPA would prove challenging. These laws primarily operate to limit profiling activity by regulating the kinds of information that can be collected, and, in some cases, how and whether the information may be disclosed. Even though some of these laws have additional requirements (for example, FCRA requires that credit reporting agencies are accurate regarding consumer credit information), none of them place meaningful restrictions on profiling activities. Profilers are not primarily interested in information disclosure or sharing, but rather in the inferences that can be drawn from information. Even laws, like FCRA, that require accuracy do not restrict the uses to which such information may be put or its downstream effects. Moreover, the narrow extent of these laws' regulatory scope to particular subject areas and definitions of "personally identifiable information" means that other identifiable information can be used to build user profiles while still remaining compliant with the law.

---

[8] The Fair Credit Reporting Act, 15 U.S.C. § 1681

[9] *See* https://caselaw.findlaw.com/us-dc-circuit/1375325.html

[10] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505

Although these sector-specific laws provide increased transparency and disclosure regarding profiling activity, transparency, in itself, does not directly prevent the profiling activity nor its harmful results.

Nevertheless, transparency remains the primary regulatory approach to profiling activities in the US. On a state level, Vermont passed the first law in the US to regulate data brokers, requiring data brokers who collect, aggregate, and sell data about Vermont residents to register on a publicly available state registry.[11] The registry requires data brokers to detail whether they have any way for consumers to opt out of the collection, and to detail any data breaches they have had in the past year. Data brokers play a significant role in the corporate profiling economy; they collect and share information about consumers from a wide variety of commercial, government, and other publicly available sources and then sell this information, in the form of marketing products (including consumer profile lists) to many third-party services (Ramirez et al., 2014). By requiring data brokers to register, Vermont is hoping to provide increased transparency about the extensive profiling activities of this otherwise-obscure part of the data market.[12]

The California Consumer Privacy Act, the recent landmark California privacy law, takes a similar approach to profiling. It provides data subjects with the right to know what personal information is being collected about them, the right to know whether their personal information is sold or disclosed and to whom, the right to opt out of the sale of their personal information, and the right to request access to the personal

---

[11] Data Broker Regulations Act, 9 V.S.A. § 2430.

[12]Additionally, several states, in the past year, have expanded their state privacy laws, including Oregon, Nebraska, Louisiana, Iowa, Arizona, Colorado, South Dakota, Alabama, Washington DC, and California. Most significantly, California passed a landmark new privacy law last year. Though negotiations about the new law is still ongoing and the law does not take effect until 2020, the draft form of the law creates several new provisions that would make it the most extensive data protection law in the US.

data collected about them.[13] Like other regulatory attempts aimed at transparency, these rights help increase awareness of corporate profiling activities and may reduce associated harms, but they do not prevent corporations from profiling. Indeed, the right to know what information is collected and sold does not necessarily help an individual understand what the harmful consequences of such collections/sales activity may be.

US consumer protection regimes also place limits on the scope of permissible contract terms between users and companies regarding the collection and use of user data. The FTC, as well as all 50 US States, prohibit companies from engaging in "unfair and deceptive acts and practices (UDAP)."[14] UDAP laws are the primary basis for regulating corporate data practices in the US, under the theory that specific uses of user data exceed the scope of the terms of collection to which users agreed to, and as such, is unfair and deceptive.

However, regulating profiling activities via consumer protection also faces significant limitations. US consumer protection law is confined to the contract the consumer signed. As a result, claims can only be brought against the entity collecting the data, not necessarily the body engaged in the profiling activity that may be harming consumers. Take the WSJ health insurance story example discussed in the introduction: suppose some of the data used by health insurers were initially collected from Venmo. As long as the sale of data to third parties by Venmo is allowed under the contract users sign with Venmo, it would be challenging to argue that the sale of such data to health insurers is unfair or deceptive. Moreover, much of Venmo data is public - making it even more challenging for consumers to claim that the subsequent use of that data for profiling purposes exceeds the contractual scope of their agreement with Venmo.

The scope of the US consumer protection's regulation of profiling may be shifting. This spring, the DETOUR Act, a bi-partisan bill from Sens. Mark Warner and Deb

---

[13] California Consumer Privacy Act, AB-375; bill text at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[14] FTC Act §5(a), 15 USC §45.

Fischer, was introduced to prohibit certain qualifying online platforms from using deceptive user interfaces, known as "dark patterns," to manipulate users and extract personal data.[15] The FTC recently fined Facebook $5 billion, the largest fine the agency has yet leveled against any technology company, for violating the terms of Facebook's 2011 privacy settlement.[16] In addition, the District of Columbia is engaged in ongoing litigation against Facebook for the sale of third-party data to Cambridge Analytica, under its UDAP laws, with other states likely to follow suit.[17] These lawsuits argue that data collectors, like Facebook, should be liable for downstream harmful consumer effects that result from the sale of data and profiling activities. If the courts accept this argument, it could significantly expand the scope of consumer protection laws to include harms arising from profiling behavior.

Anti-Discrimination Laws

The other significant way profiling activities can be regulated in the US is via anti-discrimination laws.[18] This approach does not focus on the terms of collection or on the use of user data in building out a profile, but rather on whether the profiling activity results in discrimination. US discrimination laws take two approaches: discrimination based on disparate treatment and discrimination based on disparate impact. Corporate profiling activity may be implicated in either kind of discrimination claim,

---

[15] U.S. Congress, Senate, *Deceptive Experiences To Online Users Reduction (DETOUR) Act*, SIL19435, 116th Cong., 1st Sess., introduced in Senate April 9, 2019, https://www.scribd.com/document/405606873/Detour-Act-Final

[16]United States of America v. Facebook, 19-cv-2184, Complaint for Civil Penalties, Injunction and Other Relief, (D.C. Dist. Ct.) (July 24, 2019) available along with related materials here: https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc; see also Cecilia Kang, "F.T.C. Approves Facebook Fine of About $5 Billion" New York Times, July 12, 2019.

[17] So far, states that have filed suit include the District of Columbia, see District of Columbia v. Facebook, Inc., Complaint for Violation of the Consumer Protection Procedures Act (D.C. Sup. Ct) (Dec 19, 2018)

[18] Selbst and Barocas, Big Data's Disparate Impact, 104 Cal. L. Rev. 671 (2016).

based on whether 1) the profiling activity is itself an instance of disparate treatment, or 2) the profiling activity creates a disparate impact among different groups.

Returning to the WSJ example, let us imagine that instead of health insurers, employers were using social media data to screen potential employees. If potential employers were only using social media data to screen applicants that they suspected of being foreign nationals, this may give rise to a claim of disparate treatment, since this profiling activity singles out applicants on the basis of national origin and subjects them to additional screening.[19] Alternatively, imagine an employer is screening all applicants, but this profiling results in all foreign-born applicants being excluded from consideration for employment.[20] This could give rise to a claim of disparate impact.

Regulating profiling activities via discrimination has two significant drawbacks. First, discrimination cases are difficult to prove and hard to discover, even more so in the context of online profiling. Second, relying on discrimination law to regulate profiling activity fails to provide comprehensive protection against the harms from corporate profiling. This approach only provides protection from those profiling activities that discriminate on the basis of already protected attributes, e.g., between between male and female job candidates. Other profiling behavior, such as attempting to identify or predict whether someone is at a high risk for health insurance coverage, or is likely to default on a loan, are not currently covered by discrimination law, yet may nevertheless result in other harmful impacts, including chilling effects.

---

[19] By singling out applicants on the basis of national origin (a protected category under Title VII of the 1964 Civil Rights Act) and subjecting them to an additional test or screening process, our hypothetical employer is treating these applicants differently based on their protected status. This would likely meet the legal test for a discrimination claim based on disparate impact set out in Title VII of the 1964 Civil Rights Act.

[20] By screening all applicants, our hypothetical employer is engaging in a "facially neutral employment practice." This is the legal test for a discrimination claim based on disparate impact set out in Title VII of the 1964 Civil Rights Act.

(5) Roadmap for Future Work

Based on the analyses in the previous sections, we present four focus areas for future research. These provide an agenda for research on chilling effects, both conceptually and empirically.

Focus area 1: The chilling effects of corporate profiling should be studied in more depth.

Our literature review showed how chilling effects are strongly associated with government surveillance and peer surveillance. However, chilling effects due to corporate surveillance have not received the same academic attention. As illustrated throughout this article, algorithmic profiling is an essential type of surveillance. But to date, our knowledge of how users' actions are chilled because of corporate profiling is limited. Moreover, it is uncertain, from a regulatory and normative perspective, which behavioral changes should be a regulatory or a fundamental rights concern. Therefore, we call for more research into chilling effects as a result of corporate profiling. In empirical terms, studying chilling effects is challenging for several reasons. First, chilling effects are a behavioral phenomenon with a temporal trajectory. Ideally, research on chilling effects should rely on behavioral and longitudinal data. However, such data is difficult and expensive to obtain, requiring advanced data analytical skills. Second, chilling effects are hard to isolate because the behavioral change might be caused by factors other than surveillance or profiling. Experiments, especially natural and field experiments, are therefore better suited to identify chilling effects causally. However, such experiments come with ethical problems. For example, exposing one group to a higher degree of profiling than the control group, for the purpose of testing a modification of behavior, is problematic. Third, empirical research on chilling effects needs a solid conceptual foundation. Our summary of the literature has shown that chilling effects theory, particularly when it comes to corporate profiling, is still emerging and quite dispersed. Having more solid theoretical foundations will allow for a better operationalization and measurement of chilling effects and bring scholars across disciplines into conversation. Actor–network theory could serve as a useful theoretical lens for applying these methods (Latour, 1996; Law, 2009).

Focus area 2: Corporate profiling activities and corresponding chilling effects should be studied across application domains.

Our second focus area relates to the application domain, type, and intensity of profiling. We have shown several examples of corporate profiling, based on popular media

coverage (Bergen & Surane, 2018; Scism, 2019; Valentino-DeVries et al., 2018) and academic literature (Penney, 2017). These examples include application domains such as finance (Scism, 2019), entertainment (Valentino-DeVries et al., 2018), and commerce/marketing (Bergen & Surane, 2018). Brayne (2017). Furthermore, we have further identified criminal justice, healthcare, public assistance, and employment as essential application domains. We have limited knowledge of where profiling is most prevalent and intense and where user awareness about profiling is most pronounced. Thus, comparative studies could systematically assess profiling types and intensities across application domains. Computational methods could serve to map such differences, for example via systematic access requests. In a second step, this information could be connected to user studies in terms of chilling effects. In other words, it could be tested whether the type and intensity of profiling corresponds with user awareness and (chilled) behavior.

Focus area 3: Chilling effects from corporate profiling should be studied from a social inequalities and social justice perspective.

Our third focus area relates to social justice and inequality. Recent privacy literature has shown an increased interest in social inequalities, stressing the disproportionate surveillance of disadvantaged groups (e.g., Eubanks, 2014; Madden et al., 2017; Marwick & Boyd, 2018). At the same time, algorithmic discrimination has become a topic of great concern (Noble, 2018). This is in line with the idea of social sorting in the surveillance studies literature (Lyon, 2003). While direct connections between this literature and chilling effects are apparent, they have not received the attention they deserve. Murray and Fussey (2019, p. 46) point out that "[...] it is the groups holding the fewest resources [...] that are most heavily impacted upon by chilling effects." Accordingly, we call for more focus on the entanglements between class, gender, age, and race on one hand and chilling effects due to corporate surveillance on the other hand. What does it mean in terms of democratic representation and voice when those who are already disadvantaged are disproportionately affected by profiling and therefore, particularly likely to be chilled? Action research and close collaboration between researchers and social justice groups are particularly promising avenues to address inequalities in chilling effects that result from corporate profiling. Crucially, the perspectives and expertise from those most affected are needed.

Focus area 4: Chilling effects from corporate profiling need more attention in both European and US Law

Our final focus area connects to our legal analyses in Section (4). As this analysis shows, substantial differences, but also similarities exist between European and US regulatory approaches to corporate profiling. One particularly noteworthy similarity is that, while both legal regimes are beginning to grapple with some of the harms of corporate profiling activity, none of these early responses explicitly consider the chilling effects such activity may have. To develop regulatory responses to corporate profiling activity will first require establishing empirically what current research already implies: that such profiling behavior results in the suppression of online and offline activity, resulting in concrete individual and societal harms. From such work, both US and European regimes may begin to craft adequate legal responses, with the aim of protecting individuals from harmful downstream impacts that may arise from corporate profiling based on legitimate online and offline behavior.

(6) Conclusions

In this article, we provided an overview of the literature on corporate profiling and chilling effects, with the aim of connecting the two topics. We started by explaining how profiling creates substantial power asymmetries between users and corporations (Zuboff, 2019). Particularly, we stressed the notion of inferences and the increasingly automatic nature of decision-making as essential aspects of profiling. We then discussed chilling effects in depth and connected them to corporate profiling in three ways. First, we stressed the similarities between profiling and surveillance. Second, we illustrated chilling effects as a result of state and peer surveillance—as contexts with more established evidence than chilling effects of corporate surveillance. Finally, we spotlighted the customization of behavior and behavioral manipulation as particularly significant issues in this discourse. While Section (3) approached the topic from a predominantly social science perspective, the next section was dedicated to exploring the legal foundations of profiling through an in-depth analysis of European data protection and anti-discrimination laws and US sector-specific and state laws. We found that both approaches do not sufficiently address the issues relating to the profiling activities of corporations. While there is an attempt to regulate differential impacts of profiling via anti-discrimination statutes, few policies focus on combating generalized harms of profiling, such as chilling effects. Finally, we brought the diverse strands of literature together in four focus areas to guide future research on the topic.

Our article highlights the importance of reflecting on the potential externalities of algorithmic profiling by corporations from a theoretical and practical angle. It shows the need to frame corporate profiling as a matter of concern that goes beyond just privacy and data protection, but as a potential threat to individual autonomy. Coming back to the example at the beginning of the article (WSJ, 2019), this case and similar stories (e.g., the increasingly pervasive nature of profiling and citizen scoring in China) should ring alarm bells. If individuals are increasingly aware of corporate profiling and preemptively adapt their behavior to appease profiling systems, we might find a more streamlined and competitive society, with less space for non-conformity and alternative lifestyles. Citizens who are unaware of these profiling activities would be left out of the optimization game and would be disproportionately penalized and discriminated against, for example when trying to get a loan or a new job. Thus, awareness about profiling activities and the necessary media literacy skills needed to react to them (which are likely correlated with existing markers of socioeconomic status such as education and income) could become a new axis of discrimination, exacerbating existing inequalities. The fact that the few empirical studies on the chilling effects of government surveillance found evidence for such effects (Penney, 2017; Stoycheff et al., 2018) suggests that similar mechanisms are at play with corporate profiling.

Acknowledgements

E. F. declares that part of this project was funded by the LEaDing Fellows Marie Curie COFUND fellowship, a project that has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant Agreement No. 707404. S. V. declares that part of this project was funded by the Fulbright U.S. Scholar Program.

References

Agre, P. E. (1994). Surveillance and capture: Two models of privacy. *The Information Society*, *10*(2), 101-127.

Andrejevic, M. (2004). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, 2(4), 479-497.

Article 29 Working Party (2018) Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Last revised February 6, 2018, ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826.

Barendt, E., Lustgarten, L., Norrie, K., & Stephenson, H. (1997). *Libel and the Media: The Chilling Effect*. New York: Clarendon Press.

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and Informatics*, *34*(7), 1038-1058.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26-53.

Bergen, M., & Surane, J. (2018) Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales. Bloomberg. Last modified August 30, 2018, https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales.

Bernal, P. (2016). Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy*, 1(2), 243-264.

Bosco, F., Creemers, N., Ferraris, V., Guagnin, D., & Koops, B. J. (2015). Profiling technologies and fundamental rights and values: regulatory challenges and perspectives from European Data Protection Authorities. In: Gutwirth S., Leenes R., de Hert P. (eds) *Reforming European Data Protection Law*. Law, Governance and Technology Series, Springer, 20, 3-33.

boyd, d. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi (Ed.), *A Networked Self* (pp. 47-66). London: Routledge.

Bozdag, E., & van den Hoven, J. (2015). Breaking the filter bubble: democracy and design. *Ethics and Information Technology*, *17*(4), 249-265.

Brandtzæg, P. B., Lüders, M., & Skjetne, J. H. (2010). Too many Facebook "friends"? Content sharing and sociability versus the need for privacy in social network sites. *International Journal of Human–Computer Interaction*, *26*(11-12), 1006-1030.

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review*, *82*(5), 977-1008.

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1) 1-12.

Calo, R., & Rosenblat, A. (2017). The taking economy: Uber, information, and power. *Columbia Law Review*, 1623-1690.

Čas, J., Strauss, S., Amicelle, A., Ball, K., Halliman, D., Friedewald, M., & Szekely, I. (2014). Social and economic costs of surveillance. In D. Wright & R. Kreissl (Eds.), *Surveillance in Europe* (pp. 211-258). London: Routledge.

Chen, A. (2019) Why it's time to rethink the laws that keep our health data private. *The Verge*. Last Modified January 2019. https://www.theverge.com/2019/1/29/18197541/health-data-privacy-hipaa-policy-business-science

Chen, D., Fraiberger, S. P., Moakler, R., & Provost, F. (2017). Enhancing transparency and control when drawing data-driven inferences about individuals. *Big Data*, *5*(3), 197-212. https://doi.org/10.1089/big.2017.0074.

Christl, W. (2017). Corporate surveillance in everyday life. How companies collect, combine, analyze, trade and use personal data on billions. Cracked Lab – Institute for Critical Digital Culture. Last modified June 2017, https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf.

Council of Europe (2019) Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes. Adopted by the Committee of Ministers on 13 February 2019 at the 1337th meeting of the Ministers' Deputies, https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168092dd4b.

Custers, B. (2004). The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology. Nijmegen: Wolf Legal Publishers.

Custers, B., Calders, T., Zarsky, T., & Schermer, B. (2013). The way forward. In *Discrimination and Privacy in the Information Society*, Springer, 341-357.

Das, S., & Kramer, A. (2013, June). Self-censorship on Facebook. In *Seventh international AAAI Conference on Weblogs and Social Media* (pp. 120-127). Palo Alto, CA: AAAI. Retrieved from https://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350

Dumortier F. (2010) Facebook and Risks of "De-contextualization" of Information. In: Gutwirth S., Poullet Y., De Hert P. (eds) *Data Protection in a Profiled World.* Springer, 119-137.

Dworkin, G. (1988). *The theory and practice of autonomy.* Cambridge University Press.

EU Agency for Fundamental Rights (FRA), (2018). Preventing unlawful profiling today and in the future: a guide. Available at: https://fra.europa.eu/en/publication/2018/prevent-unlawful-profiling.

Eubanks, V. (2014). Want to predict the future of surveillance? Ask poor communities. The *American Prospect*, 15 January 2014. Retrieved from https://prospect.org/article/want-predict-future-surveillance-ask-poor-communities

Eurobarometer (EB) 359, Data Protection and Electronic Identity in the EU (2011), available at: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf

Fair, L. (2011). The Fair Credit Reporting Act & social media: What businesses should know. Federal Trade Commission. Last Modified June 2011. https://www.ftc.gov/news-events/blogs/business-blog/2011/06/fair-credit-reporting-act-social-media-what-businesses.

Fox, J., & Warber, K. M. (2014). Queer identity management and political self-expression on social networking sites: A co-cultural approach to the spiral of silence. *Journal of Communication*, *65*(1), 79-100.

Gandy Jr, O. H. (2006). Data mining, surveillance, and discimination in the post-9/11 environment. *The New Politics of Surveillance and Visibility* (pp. 363-384). University of Toronto Press.

Gandy, O. (2012). Statistical surveillance: Remote sensing in the digital age. In: Ball KS, Haggerty K and Lyon D (eds) *Routledge Handbook of Surveillance Studies*. (pp. 125–132). London: Routledge.

George, D., Reutimann, K., 6 Tamò-Larrieux, A. (2018). GDPR Bypass by Design? Transient Processing of Data Under the GDPR (August 9, 2018). Retrieved from https://ssrn.com/abstract=3243389 or http://dx.doi.org/10.2139/ssrn.3243389

Graf, E. (2017). When automated profiling threatens our freedom: A Neo-Republican perspective. *European Data Protection Law Review. 3*(4) 441-451.

Hampton, K. N., Rainie, H., Lu, W., Dwyer, M., Shin, I., & Purcell, K. (2014). Social media and the 'spiral of silence'. *Pew Research Center: Internet & Technology*, 26 August 2014. Retrieved from http://www.pewinternet.org/2014/08/26/social-media-and-the-spiral-of-silence/

Hanson, J. D., & Kysar, D. A. (1999). Taking behavioralism seriously: The problem of market manipulation. *New York University Law Review, 74*, 630-750.

Hildebrandt, M. (2008). Defining Profiling: A New Type of Knowledge. In M. Hildebrandt and S. Gutwirth (Eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*. Springer, 17-30.

Hogan, B. (2010). The presentation of self in the age of social media: Distinguishing performances and exhibitions online. *Bulletin of Science, Technology & Society, 30*(6), 377-386.

Holloman, C. (2014) Your Facebook updates now determine your credit score. The Guardian. Last modified, August 28, 2014, https://www.theguardian.com/media-network/media-network-blog/2014/aug/28/social-media-facebook-credit-score-banks.

Kamarinou, D., Millard, C., Singh J. (2017). "Machine Learning with Personal Data", in: R. Leenes, R. van Brakel, S. Gutwirth, & P. De Hert (eds.), *Data Protection and Privacy: The Age of Intelligent Machines*, Hart Publishing, 89-114.

Kandias, M., Mitrou, L, Stavrou, V., Gritzalis, D. (2016). Profiling Online Social Networks users: An Omniopticon tool, *International Journal of Social Networks Mining*, *2*(4), 293-313.

Kim, S.-H., Kim, H., & Oh, S.-H. (2014). Talking about Genetically Modified (GM) foods in South Korea: The role of the Internet in the spiral of silence process. *Mass Communication and Society*, *17*(5), 713-732.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122-134.

Koops, B. J. (2008). Some reflections on profiling, power shifts, and protection paradigms. In M. Hildebrandt, & S. Gutwirth (Eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (pp. 326-337). Amsterdam: Springer.

Latour, B. (1996). On actor-network theory: A few clarifications. *Soziale Welt*, *47*(4), 396-381.

Law, J. (2009). Actor network theory and material semiotics. In B. S. Turner (Ed.), *The New Blackwell Companion to Social Theory* (pp. 141-158). Hoboken, NJ: Wiley.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.

Le Métayer, D., & Le Clainche, J. (2012). From the protection of data to the protection of individuals: extending the application of non-discrimination principles. In European Data Protection: In Good Health? Springer, 315-329.

Levitin, A. (2018). Facebook: the new Credit Reporting Agency? Credit Slips. Last Modified August 2018, https://www.creditslips.org/creditslips/2018/08/facebook-the-new-credit-reporting-agency.html.

Lyon, D. (2001). Surveillance Society, Monitoring everyday life. Open University Press.

Lyon, D. (2003). Surveillance as social sorting: Computer codes and mobile bodies. In D. Lyon (Ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (pp. 13-30). London: Routledge.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1-13.

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and Big Data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review*, *95*, 53-126.

Manokha, I.(2018). Surveillance, Panopticism, and Self-Discipline in the Digital Age. *Surveillance & Society, 16(2),* 219-237.

Mantelero, A. (2014). The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. *Computer Law & Security Review,* 30(6), 643-660.

Marder, B., Joinson, A., Shankar, A., & Houghton, D. (2016). The extended 'chilling' effect of Facebook: The cold reality of ubiquitous social networking. *Computers in Human Behavior, 60,* 582-592.

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society, 13*(1), 114-133.

Marwick, A., & boyd, d. (2018). Understanding privacy at the margins. *International Journal of Communication, 12,* 1157-1165.

Marthews, A., & Tucker, C. (2017). The Impact of Online Surveillance on Behavior. In D. Gray & S. Henderson (Eds.), *The Cambridge Handbook of Surveillance Law* (Cambridge Law Handbooks) Cambridge University Press, 437-454.

Micheli, M., Lutz, C., & Büchi, M. (2018). Digital footprints: an emerging dimension of digital inequality. *Journal of Information, Communication and Ethics in Society, 16*(3), 242-251.

Mitrou, L., Kandias, M., Stavrou, V., Gritzalis, D. (2014). Social media profiling: A Panopticon or Omniopticon tool? In *Proceedings of the 6th Conference of the Surveillance Studies Network.* Retrieved from https://www.infosec.aueb.gr/Publications/2014-SSN-Privacy%20Social%20Media.pdf.

Murray, D., & Fussey, P. (2019). Bulk surveillance in the digital age: Rethinking the human rights law approach to bulk monitoring of communications Data. *Israel Law Review, 52*(1), 31-60.

New York Times (2018). The business of selling your data. Last modified 10 December, 2018, https://www.nytimes.com/2018/12/10/podcasts/the-daily/location-tracking-apps-privacy.html.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79,* 101–139.

Noble, S. (2018). *Algorithms of Oppression.* New York University Press.

Noelle-Neumann, E. (1974). The spiral of silence a theory of public opinion. *Journal of Communication, 24*(2), 43-51.

Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.

Penney, J. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review, 6*(2), 1-39.

Petkova, B. & Boehm, F. (2018). Profiling and the Essence of the Right to Data Protection. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge Handbook of Consumer Privacy* (Cambridge Law Handbooks, pp. 285-300). Cambridge: Cambridge University Press. doi:10.1017/9781316831960.017

Raley, R. (2013). Dataveillance and countervailance. In L. Gitelman (Ed.), *'Raw Data' is an Oxymoron* (pp. 121-146). Cambridge, MA: MIT Press.

Ramirez, E., Brill, J., Ohlhausen, M., Wright, J. , McSweeny, T. (2014). Report: Data Brokers: A Call for Transparency and Accountability. Federal Trade Commission. Last modified May 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Rao, A., Schaub, F., & Sadeh, N. (2015). What do they know about me? Contents and concerns of online behavioral profiles. Retrieved from https://arxiv.org/abs/1506.01675.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1).

Reece, A., & Dandforth, C. (2017). Instagram photos reveal predictive markers of depression. *EPJ Data Science, 6*, 1-15.

Renas, S. M., Hartmann, C. J., & Walker, J. L. (1989). An Empirical Analysis of the Chilling Effect. In E. E. Dennis & E. M. Noam (Eds.), *The Cost of Libel: Economic and Policy Implications.* Columbia University Press, 41-68.

Sax, M. (2016). Big data: Finders keepers, losers weepers? *Ethics and Information Technology, 18*(1), 25-31.

Schauer, F. (1978). Fear, risk and the first amendment: Unraveling the chilling effect. *Boston University Law Review, 58*, 685-732.

Schermer, B. (2011). The limits of privacy in automated profiling and data mining. *Computer Law and Security Review, 27*, 45-52.

Schneier, B. (2013). The Public-Private Surveillance Partnership. Bloomberg Opinion. Last modified August 1, 2013, https://www.bloomberg.com/opinion/articles/2013-07-31/the-public-private-surveillance-partnership

Schreurs, W., Hildebrandt, M., Kindt, E., & Vanfletern, M. (2008). Cogitas Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group profiling in the Private Sector. In M. Hildebrandt & S. Gutwirth (Eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (241-264). Amsterdam: Springer.

Scism, L. (2019). New York Insurers Can Evaluate Your Social Media Use—If They Can Prove Why It's Needed. *Wall Street Journal.* Last modified, January 30, 2019, https://www.wsj.com/articles/new-york-insurers-can-evaluate-your-social-media-useif-they-can-prove-why-its-needed-11548856802

Schütz, A. (1998). Assertive, offensive, protective, and defensive styles of self-presentation: A taxonomy. *The Journal of Psychology*, *132*(6), 611-628.

Solove, D. (2006) A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477-488.

Solove, D. (2007) The First Amendment as criminal procedure. *New York University Law Review*, *82*(1), 112-155.

Speicher, T., Ali, M., Venkatadri, G., Ribeiro, F. N., Arvanitakis, G., Benevenuto, F., … Mislove, A. (2018). Potential for discrimination in online targeted advertising. *Conference on Fairness, Accountability and Transparency*, (pp. 5-19). Retrieved from http://proceedings.mlr.press/v81/speicher18a.html

Stark, L. (2018) Start treating private personal data on Facebook like medical data: It's just as sensitive to nefarious manipulation. Daily News. Last modified March 2018, https://www.nydailynews.com/opinion/start-treating-private-personal-facebook-data-medical-data-article-1.3891871.

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA Internet monitoring. *Journalism & Mass Communication Quarterly*, *93*(2), 296-311.

Stoycheff, E., Liu, J., Xu, K., & Wibowo, K. (2018). Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects. *New Media & Society 21*(3), 602-619.

Susser, D., Roessler, B., & Nissenbaum, H. (2018). Online manipulation: Hidden influences in a digital world. Retrieved from https://ssrn.com/abstract=3306006.

Symons, T., & Bass, T. (2017). Me, my data and I: The future of the personal data economy. *European Union, H2020.* Retrieved from https://pilab.nl/onewebmedia/decode-02.pdf.

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, 4(2), 2053951717736335.

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday*, *19*(7).

Valentino-DeVries, J., Singer, N., Keller, M. H., & Krolik, A. (2018) Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret. *New York Times.* Last modified, December 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197-208.

Wachter, S. (2019). Data Protection in the Age of Big Data, Nature Electronics Vol. 2, 6–7 (2019), DOI: 10.1038/s41928-018-0193-y. Retrieved from https://ssrn.com/abstract=3355444

Wachter, S. & Mittelstadt, B. (2018). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (October 5, 2018). *Columbia Business Law Review, 2019*(2). Retrieved from https://ssrn.com/abstract=3248829

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law, 7*(2), 76-99.

Wallach, H. (2018). Computational social science ≠ computer science + social data. *Communications of the ACM, 61*(3), 42-44.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & Society, 16*(4), 479-500.

Yun, G. W., & Park, S. Y. (2011). Selective posting: Willingness to post a message online. *Journal of Computer-Mediated Communication, 16*(2), 201-227.

Zarsky, T. Z. (2019). Privacy and manipulation in the digital age. *Theoretical Inquiries in Law, 20*(1), 157-189.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. London, UK: Profile Books.