Before the

National Telecommunications and Information Administration

Washington, DC

WC Docket No. 180821780–8780–01

In the Matter of

Developing the Administration's Approach to Consumer Privacy

Comment by Malte Möser

Friday, November 9, 2018

My name is Malte Möser, I am a graduate researcher in the Security and Privacy Group in the Department of Computer Science at Princeton University and a Graduate Student Fellow at the Center for Information Technology Policy (CITP).

I am writing this comment in support of stronger consumer privacy protections beyond notice and consent that better align data use practices with users' expectations and intentions. To this end, new privacy protections should protect consumers from a company's ability to influence their choices towards unintended information disclosure. Critically, outcomes and goals (and ultimately new privacy rules) should be formulated such that they achieve these aims without depending on a company's individual assessment of context or risk.

My position is derived from two main observations from empirical and behavioral privacy research:

1. Current data collection practices often violate consumers' expectations and intentions.

2. Companies are in advantageous position to influence users' privacy choices.

Current data collection practices often violate consumers' expectations.

Today, many companies base their business model upon the large-scale collection of user preferences and behavior for targeted advertising. This unprecedented amount of data collection is conducted through a variety of platforms and products: On the web, users are tracked by platforms directly (e.g., when using Facebook), as well as through third-party tracking (e.g., when another websites embeds a Facebook widget that sends back data to the platform).[1] Consumers are also increasingly tracked when using applications on their smartphones[2] or reading emails[3], and the trend is moving towards combining this data with real-world tracking (e.g., through RFID or Bluetooth beacons in stores). Furthermore, data from different sources is combined to create a more holistic picture of the user, and these enriched data sets are sold to other companies and data brokers.

---

[1] Englehardt, Steven, and Arvind Narayanan. "Online tracking: A 1-million-site measurement and analysis." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016.

[2] Razaghpanah, Abbas, et al. "Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem." Network and Distributed Systems Security (NDSS) Symposium (2018).

[3] Englehardt, Steven, Jeffrey Han, and Arvind Narayanan. "I never signed up for this! Privacy implications of email tracking." Proceedings on Privacy Enhancing Technologies 2018.1 (2018): 109-126.

Most of this tracking is happening in the background, invisible to the user. Therefore, most users have limited awareness that it is taking place at all, and thus also have limited ability to make conscious choices about it. Economists call this type of market failure an information asymmetry: one side possesses significantly more information and is thus in a more powerful position when doing business.

Current privacy procedures of notice and consent, with the notice usually being formalized in a privacy policy, are highly ineffective and do not help to remove these information asymmetries. Surveys have shown that most users just do not read privacy policies[4]. Even worse, in another survey 62% of respondents incorrectly believed that the presence of a privacy policy would prevent a company from sharing personal information without explicit permission.[5] Furthermore, the practice of notice and consent does not lead to a reduction in data collected, or give the user much of a chance to opt out of specific types of data collection.

As a result, we see more and more users upset and taken by surprise when they become aware of companies' data collection and use practices. One notable example is the recent discussion about the website "unroll.me". This free service allows users to easily unsubscribe from email subscriptions they no longer desire. To use it, users need to give the company access to their email accounts. What surprised and upset many users was that unroll.me, against users expectations, would not only analyze emails to identify potential subscription cancellations, but would also extract information related to users' online commerce and purchase activities and sell it to other companies. In one such case, unroll.me sold information about users' ride histories on the ride-sharing platform Lyft to that platform's competitor Uber.[6]

---

[4] Jensen, Carlos, Colin Potts, and Christian Jensen. "Privacy practices of Internet users: self-reports versus observed behavior." International Journal of Human-Computer Studies 63.1-2 (2005): 203-227.

[5] Hoofnagle, Chris Jay, and Jennifer M. Urban. "Alan Westin's privacy homo economicus." Wake Forest L. Rev. 49 (2014): 261.

[6] Isaac, Mike. "Uber's C.E.O. Plays With Fire." 2018. Available online at https://www.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html, retrieved on 10/16/2018.

Privacy decisions are inherently complex and involve tradeoffs. Companies can use their power to influence these decisions.

Consumers nowadays must make choices that have implications for their privacy in a variety of different contexts and on many different platforms. Making these choices efficiently requires users to make tradeoffs: they balance privacy against other needs, such as urgency or convenience. Furthermore, misperceptions, social norms or emotions all have an influence on users' choices.[7] The result is a so-called "privacy paradox": users' choices and actions do not always reflect their intentions and underlying attitudes towards privacy.

A well-known study published in 2012 by researchers at Columbia University evaluated the mismatch between users' intention to share specific types of content (e.g., photos, links or events) with certain groups of users (e.g., friends, friends of friends, strangers).[8] First, the study asked participants with whom they intended to share each type of content on the platform. Then, they analyzed whether users' actual sharing behavior matched their intentions using a Facebook application that analyzed the privacy settings of each post on a user's profile page. The study found a staggering mismatch between users' intentions and their actions: 94% had made content available to other users from whom they intended to hide it, and 85% had hidden content from an audience with whom they intended to share it.

This study highlights two important issues: users are routinely overwhelmed with the challenge to manage their privacy settings, and default settings often are not set such that they minimize a user's risk to exposure. The latter is not a coincidence or something that will improve over time. If anything, companies have an incentive to make privacy choices hard and thereby influence consumers to reveal more information than they would do otherwise. Influencing users can be done in a variety of ways, e.g., users are more likely to reveal information if they observe others reveal such information beforehand.[9] This risk of malleability has nowadays motivated researchers to study so-called "dark patterns" or

---

[7] Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. "Privacy and human behavior in the age of information." Science 347.6221 (2015): 509-514.

[8] Madejski, Michelle, Maritza Johnson, and Steven M. Bellovin. "A study of privacy settings errors in an online social network." IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). IEEE, 2012.

[9] Acquisti, Alessandro, Leslie K. John, and George Loewenstein. "The impact of relative standards on the propensity to disclose." Journal of Marketing Research 49.2 (2012): 160-174.

"malicious" interface design, to shed more light on this increasingly common attempt to influence users in unconscious ways.[10]

Often, unintuitive and confusing privacy settings prevent the user from making effective privacy choices and thereby lead them to unintended disclosure of sensitive information. The recent public outcry about Google's location privacy settings serves as a good example for such commonly occurring mismatches between users intentions and their actions.[11] Google allows users to deactivate its "Location History", a feature that tracks a user's location over time. Deactivating the location history, however, did not completely stop Google from tracking users' location, as one would expect. Instead, users would also need to disable "Web and App Activity" as well as device-level "Location Services".

New privacy protections must rebalance the asymmetries between users and companies.

The provided insights show that we need stronger privacy protections for users. These privacy protections should be aligned with users' expectations and preferences, and rebalance the information asymmetries and power imbalances between users and companies. To this end, privacy protections should provide concrete limits on the data collection and use practices of companies. A company-centric and risk-based approach, as imagined in the administration's approach to consumer privacy, would likely fall short of such protections. For one, risk is inherently hard to define and measure, and when assessed by a company might not take into account the interconnected nature of data use and abuse in practice. Furthermore, as companies already try to influence users towards unintended disclosure of personal information, privacy protections should be centered on the user and not left for companies to decide. The administration should thus consider adopting an approach to consumer privacy that provides a high baseline of privacy for consumers without depending on a company's individual assessment of context and risk.

---

[10] Conti, Gregory, and Edward Sobiesk. "Malicious interface design: exploiting the user." Proceedings of the 19th international conference on World wide web. ACM, 2010.

[11] Ryan Nakashima. "AP Exclusive: Google tracks your movements, like it or not." 2018. Available online at https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb, retrieved on 10/16/2018.