WHY COLLECTION MATTERS

SURVEILLANCE AS A DE FACTO PRIVACY HARM

Justin Brookman and G.S. Hans*

Consumer privacy remains one of the most pressing issues in technology policy. The interactions between individuals and service providers generate a great deal of data, much of it personally identifiable and sensitive. Individual users are transacting more and more data online with each passing year, and companies have begun exploring what insights and lessons they can glean from consumer data, via storage, processing, and analysis of exceedingly large data sets. These practices, loosely described as *big data*, have raised questions regarding the appropriate balance of control between individuals and companies, and how best to protect personal privacy interests.

In terms of privacy protection, some theorists have insisted that advocates must articulate a concrete harm as a prerequisite for legislated rules, or even self-regulation. Others have argued that privacy protections should focus exclusively on curtailing controversial uses rather than on the collection of personal information.

This paper argues that consumers have a legitimate interest in the mere collection of data by third parties. That is, big data collection practices *per se*, rather than bad uses or outcomes, are sufficient to trigger an individual's privacy interests.[1] Today, big data collection practices are for the most part unregulated. As collection, retention, and analysis practices become increasingly sophisticated, these threats will only increase in magnitude, with a concomitant chilling effect on individual behavior and free expression.

I. The Interests Implicated by Data Collection

Commercial collection of personal information necessarily implicates a range of potential threats that should be considered when evaluating the need for collection limitations. This paper focuses on five particular threat models: data breach, internal misuse, unwanted secondary use, government access, and chilling

* Justin Brookman is Director of Consumer Privacy at the Center for Democracy & Technology. G.S. Hans is the 2012-14 Ron Plesser Fellow at the Center for Democracy & Technology.

[1] Setting aside entirely the issue of whether consumers have privacy *rights* over their data, which this paper does not address.

effect on consumer behavior. These scenarios are for the most part outside corporate control — and indeed, contrary to corporate interest — and can never be fully mitigated by internal procedures. As big data becomes more pervasive, the susceptibility of consumer data to these threats will undoubtedly increase.

A. Data Breach

One of the most common threats that arise from the mere collection of personal information is data breach. Companies consistently experience data breaches, either due to inadequate security or aggressive external hacking. As companies collect an increasing amount of data and retain it for future uses, the consequences of a breach become more severe — both for the company and for consumers. Moreover, the more robust a company's database is, the more appealing it may be for malicious actors. The risk of breach will necessarily increase as companies collect more data about their consumers.

The consequences of data breach are obvious. Personal information, including real name, contact information, financial information, health data, and other sensitive data, can fall into the wrong hands. Consumers can therefore become susceptible to financial fraud or inadvertent identification by third parties. However, this interest extends beyond the potential for economic loss; data breach could also reveal private, embarrassing information that a consumer did not want shared with others or published to the world. For this reason, the Federal Trade Commission has increasingly found substantial harm arising from less sensitive disclosures, such as "revealing potentially embarrassing or political images"[2] "impair[ing consumers'] peaceful enjoyment of their homes,"[3] allowing hackers to "capture private details of an individual's life,"[4] and "reduc[ing consumers'] ability to control the dissemination of personal or proprietary information (e.g., voice recordings or intimate photographs)."[5]

[2] Facebook Inc., Docket No. C-4365, File No. 0923184 (Fed. Trade Comm'n July 27, 2012) (complaint), http://www.ftc.gov/os/caselist/0923184/120810facebookcmpt.pdf.

[3] Aspen Way Enterprises, Inc., Docket No. C-4392, File No. 1123151 (Fed. Trade Comm'n Apr. 15, 2013) (complaint), http://www.ftc.gov/os/caselist/1123151/aspenway/130415aspenwaycmpt.pdf.

[4] HTC America Inc., File No. 122 3049 (Fed. Trade Comm'n February 22, 2013) (complaint), http://www.ftc/gov/os/caselist/1223049/130222htccmpt.pdf.

[5] Frostwire LLC, Docket No. 23643 , File No. 112 3041(Fed. Trade Comm'n October 11, 2011) (complaint), http://www.ftc.gov/os/caselist/1123041/111011frostwirecmpt.pdf.

B. Internal Misuse

Internal misuse by rogue employees — data voyeurism — is another significant threat implicated by commercial collection of personal data. While the scale of such misuse of data would probably be markedly smaller than a data breach (which would likely be conducted by an external party), employees may possess a more focused desire to access individualized data than external hackers. For example, in one prominent case, an engineer spied on the user accounts of multiple minors, including contact lists, chat transcripts, and call logs, and used that information to manipulate the users whose accounts he had accessed.[6] Consumer reliance on cloud services to store and transmit their personal communications necessarily involves an opportunity for rogue individuals employed by those cloud services to access such data, unless the data is fully encrypted, and the companies do not have access to the encryption keys.

C. Unwanted Secondary Usage and Changes in Company Practices

Companies that collect personal information may decide to use that information in ways that are inimical to consumers' interests. Such usage could range from the merely annoying (say, retargeted advertising) to price discrimination to selling the information to data brokers who could then use the information to deny consumers credit or employment.

Even if companies do not engage in such unwanted uses right away, they may subsequently change their minds. Although the FTC has asserted for years that material retroactive changes to privacy policies constitutes deceptive and unfair business practices,[7] that legal theory has only rarely been tested in court. Moreover, in the United States, companies are not legally required to justify and explain all data usage practices at the time of collection. Companies could in a privacy policy reserve broad rights to utilize data (or potentially just remain silent on the issue), and subsequently repurpose that information without providing notice or an opportunity to opt out of such usage to the user.

---

[6] Adrian Chen, *GCreep: Google Engineer Stalked Teens, Spied on Chats*, Gawker (Sept. 14, 2010, 3:26 PM) http://gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats

[7] Gateway Learning Corp., File No. 042-3047, (Fed. Trade Comm'n September 17, 2004) (complaint), http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf.

D. Government Access

Government access without robust due process protection is arguably the most significant threat posed by the collection of personal information. As the recent NSA revelations aptly demonstrate, much of the data that governments collect about us derives not from direct observation, but from access to commercial stores of data. Even in so-called rule of law jurisdictions such as the United States and Europe, that data is often obtained without transparent process, and without a particularized showing of suspicion — let alone probable cause as determined by an independent judge. Unfortunately, there is almost nothing that consumers can do to guard against such access or in many cases even know when it occurs.[8]

E. Chilling Effects

Finally, all these concerns together —along with others, and even with an irrational or inchoately realized dislike of being observed — has a chilling effect on public participation and free expression. Consumers who don't want to be monitored all the time may be resistant to adopting new technologies; indeed, the Obama administration used this as an explicit commercial justification in calling for the enactment of comprehensive commercial privacy protections.[9]

More fundamentally, however, citizens who fear that they are being constantly observed may be less likely to speak and act freely if they believe that their actions are being surveilled. People will feel constrained from experimenting with new ideas or adopting controversial positions. In fact, this constant threat of surveillance was the fundamental conceit behind the development of the Panopticon prison: if inmates had to worry all the time that they were being observed, they would be less likely to engage in problematic behaviors.[10] Big Data transposes this coercive threat of constant observation to everyday citizens.

The United States was founded on a tradition of anonymous speech. In order to remain a vibrant and innovative society, citizens need room for the expression of controversial —

[8] For a more expansive exploration of the privacy threats implicated by government surveillance, *see* Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (2011).

[9] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, February 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[10] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (1977).

and occasionally wrong — ideas without worry that the ideas will be attributable to them in perpetuity. In a world where increasingly every action is monitored, stored, and analyzed, people have a substantial interest in finding some way to preserve a zone of personal privacy that cannot be observed by others.

II. Internal Controls Are Necessary — But Not Sufficient

When faced with these threat models, some have argued that they can be sufficiently addressed by internal organizational controls — such as privacy by design, accountability mechanisms, and use limitations. However, of the above threats, only unwanted secondary usage can be fully solved by internal controls, as deliberate secondary usage is the only threat model fully within the control of the organization. Even then, if the data is retained, the organization could eventually change its mind if the internal controls weaken, ownership is transferred, or the organization is dissolved and its assets liquidated.[11]

Data breach, internal misuse, and government access all derive from extra-corporate motivations, and cannot be definitively prevented so long as the data remains within the company's control. Adherence to best practices and strict protections can diminish the threat of data breach and internal misuse, but cannot wholly prevent them. When it comes to government access, internal controls are even less effective. Companies may engage in heroic efforts to prevent disclosure of customer records, but ultimately they can be beholden by law to comply.[12]

Empirically, internal privacy programs have proven to be insufficient to prevent privacy violations. Many of the companies cited to date by the FTC, state Attorneys General, and private suits have been large companies with mature and far-ranging privacy compliance mechanisms in place. Despite these state-of-the-art programs, those companies either lost control of the data or internally justified privacy-invasive practices.

Moreover, internal controls are completely opaque and indistinguishable to the average user, rendering them rather ineffective in diminishing the chilling effect of surveillance. However, as noted above, even if consumers could discern and

[11] Toysmart.com, LLC, Docket No. 00-11341-RGS, File No. X000075 (Fed. Trade Comm'n July 21, 2000) (complaint), http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm.

[12] Claire Cain Miller, *Secret Court Ruling Put Tech Companies in Data Bind*, N.Y. Times (June 14, 2013), at A1, *available at* http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-data-bind.html.

evaluate the full range of internal controls over their data, their fears would not be assuaged.[13]

III. Conclusion

The ambition of this paper is deliberately modest. We merely endeavor to articulate (beyond allegations of *creepiness*) why consumers have a privacy interest in controlling commercial collection of their personal information, rather than relying entirely on best practices in use limitations. We do not mean to argue that this interest should always outweigh legitimate commercial interests in that same data, or that consumers' interest always necessitates express consent for all data collection. However, it is an important interest, deserving of consideration in evaluating the appropriate framework for commercial data protection.

[13] Which is not to say that internal controls are not privacy-enhacing, or indeed essential, to preserving data that has been collected. Moreover, some internal controls are more effective than others. Data deletion (and to a lesser extent aggregation and anonymization) is almost certainly the most effective internal control in eliminating the privacy threat posed by static stores of consumer data. Even then, consumers likely have imperfect visibility into internal deletion practices, and may not fully trust in the adequacy of companies' deletion or deidentification techniques. That said, strong data deletion policies are probably the most effective way to address the harms of collection after the fact.