Corporate privacy policy changes during PRISM and the rise of surveillance capitalism

Kumar, Priya

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Kumar, P. (2017). Corporate privacy policy changes during PRISM and the rise of surveillance capitalism. *Media and Communication*, *5*(1), 63-75. https://doi.org/10.17645/mac.v5i1.813

COGITATIO

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 63–75
DOI: 10.17645/mac.v5i1.813

Article

Corporate Privacy Policy Changes during PRISM and the Rise of Surveillance Capitalism

Priya Kumar

College of Information Studies, University of Maryland, College Park, MD 20742, USA; E-Mail: pkumar12@umd.edu

Submitted: 25 October 2016 | Accepted: 28 November 2016 | Published: 22 March 2017

Abstract
Disclosure of the NSA's PRISM program demonstrated that Internet companies have become prime targets of government surveillance. But what role do companies themselves play in putting users' privacy at risk? By comparing the changes in the privacy policies of ten companies—the nine in PRISM plus Twitter—I seek to understand how users' privacy shifted. Specifically, I study how company practices surrounding the life cycle of user information (e.g. collection, use, sharing, and retention) shifted between the times when companies joined PRISM and when PRISM news broke. A qualitative analysis of the changes in the privacy policies suggests that company disclosure of tracking for advertising purposes increased. I draw on business scholar Shoshana Zuboff's conceptualization of "surveillance capitalism" and legal scholar Joel Reidenberg's "transparent citizen" to explain the implications such changes hold for users' privacy. These findings underscore why public debates about post-Snowden privacy rights cannot ignore the role that companies play in legitimizing surveillance activities under the auspices of creating market value.

Keywords
Internet companies; PRISM; privacy policies; surveillance capitalism; targeted advertising; transparent citizen

Issue
This article is part of the issue "Post-Snowden Internet Policy", edited by Julia Pohle (WZB Berlin Social Science Center, Germany) and Leo Van Audenhove (Vrije Universiteit Brussel, Belgium).

1. Introduction: The Relationship between Government and Corporate Surveillance

In August 2016, New Zealander Tony Fullman became "the first person in the world to be publicly identified as a confirmed" target of the NSA's PRISM surveillance program (Gallagher & Hager, 2016). Intelligence officials in New Zealand believed Fullman and others were concocting a plot to violently overthrow Fiji's authoritarian leader. According to documents that Edward Snowden provided to The Intercept, an investigative news outlet, the U.S. National Security Agency (NSA) used PRISM to access Fullman's Gmail and Facebook accounts and turned over more than 190 pages of his communication and private information, such as bank statements, to New Zealand authorities. The information revealed no evidence of a plot, and ultimately, the government never brought charges against Fullman or others it investigated (Gallagher & Hager, 2016).

While governments are certainly justified in investigating credible threats of violence, The Intercept's investigation suggests that even before New Zealand's authorities received Fullman's communications from the NSA, they had scant evidence that the plot to assassinate Fiji's leader was, in fact, credible. Fullman exemplifies the "transparent citizen" (Reidenberg, 2015). By using networked digital technologies now common in everyday life, he becomes increasingly visible to institutional actors like governments and companies, yet those institutions' use of his personal information remains obscure. The rise of a transparent citizenry threatens privacy, undermines trust in rule of law, and challenges international norms and data flows (Reidenberg, 2015). PRISM targets non-U.S. persons located outside of the U.S., but a report from the U.S. Privacy and Civil Liberties Oversight Board ([PCLOB], 2014) found that aspects of the program also present privacy concerns for U.S. persons.

PRISM is a top-secret intelligence program in which the NSA can compel U.S.-based companies to provide information associated with certain "selectors", such as an email address or phone number. Selectors cannot include individual names or other key words (PCLOB, 2014). The Snowden disclosures name nine U.S.-based company partners: Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, Skype, AOL, and Apple (Gellman & Poitras, 2013). The program stems from legal authority Congress granted to the U.S. government under Section 702 of the Foreign Intelligence Surveillance Act Amendments Act of 2008. The PCLOB reviewed PRISM and other surveillance programs operating under the aegis of Section 702 and concluded, "PRISM collection is clearly authorized by the statute" (PCLOB, 2014, p. 9). Nevertheless, privacy and surveillance lawyers argue that Section 702's overbroad scope and insufficient protections, combined with the government's lack of transparency regarding the operations of surveillance programs authorized under Section 702, threaten the privacy and civil liberties of those within and beyond the U.S. (Butler & Granick, 2016). In 2015, the Court of Justice of the European Union invalidated the Safe Harbor agreement that permitted U.S. companies to transfer the personal data of E.U. citizens into the U.S. The court cited concerns with the U.S. surveillance programs described in Snowden's disclosures, including PRISM (Ni Loideain, 2016).

The Snowden disclosures re-ignited a public conversation about the extent to which governments should access data that people generate in the course of their daily lives. The act of governments obtaining data from third parties such as companies is nothing new. However, the rise of cloud computing and pervasive computing coupled with inexpensive data storage has enabled companies to store and retain increasing amounts of data, giving governments more data to pursue (Bellia, 2008). Indeed, "government and nongovernment surveillance support each other in a complex manner that is often impossible to disentangle" (Richards, 2013, p. 1940). Of course, companies do not collect and store user information with the goal of sharing it with the government. Rather, the allure of big data entices companies to collect and retain as much data as they can. Analyzing that data enables companies to predict and modify human behavior while also generating revenue and market control. Such is the logic of surveillance capitalism, "a new social relations and politics that have not yet been well delineated or theorized" (Zuboff, 2015, p. 76).

In the wake of Snowden's disclosures, several companies denied giving the U.S. government "direct access" to their servers, as PRISM was mistakenly first reported to entail (Blodget, 2013). However, companies are legally required to respond to national security demands, such as those the government makes under PRISM, and in some cases, companies facilitated this process (Miller, 2013). Important debate continues about the legality of Section 702, which authorizes PRISM and other surveillance programs (Butler & Granick, 2016). I argue that, in addition to interrogating the legality of surveillance frameworks, conversations regarding post-Snowden Internet policy must also examine the degree to which companies' own business practices can legitimate surveillance of Internet users around the world.

Why study these companies? The nine U.S. companies named in Snowden's PRISM disclosures are by no means the only ones who engage in and benefit from surveillance capitalism. And while disclosure of PRISM certainly spotlighted these companies, several companies had already attracted significant public and regulatory attention due to privacy concerns before the news broke. Nevertheless, the U.S. government's decision to explicitly include them in a secret surveillance program suggests that their data holds particular value and that their business practices related to that data deserve closer examination. These companies collectively serve billions of Internet users around the world, meaning they hold the power to respect or imperil the privacy rights of many (MacKinnon, 2012).

In this vein, I analyze the changes in company privacy policies over two time frames to understand how users' privacy rights shifted since companies entered PRISM. I focus on one aspect of privacy—the flow of user information across the "the informational life cycle", (Schwartz & Solove, 2014, p. 892), which includes the collection, use, sharing, and retention of user information (Kumar, 2016). This translates to the following research question:

> How did company practices surrounding the life cycle of user information (its collection, use, sharing, and retention) change in the time period spanning companies' entrance into PRISM and the program's disclosure to the public?

I don't contend that PRISM caused the companies to change their privacy policies. I suggest that while they were part of PRISM, companies undermined their users' privacy rights by expanding their use of targeted advertising, which is tantamount to tracking their users. This offers evidence of the rise of surveillance capitalism, where companies have business incentives to aggregate more and more user information, and governments gain an attractive trove of data to access for surveillance purposes. The next section of this paper describes the various stakeholders that influence company actions and outlines this paper's conception of users' privacy rights online. Section 3 explains the methods I used to locate and analyze company privacy policies. Section 4 reviews privacy policy changes related to the life cycle of user information, and sections 5 and 6 examine what this analysis contributes to debates about privacy rights in a post-Snowden world.

2. The Role of Companies in Respecting Users' Online Privacy Rights

Encouraging companies to act in ways that respect their users' privacy is a complex endeavor. Companies are ac-

countable to several stakeholders: investors expect maximized returns and minimized risk; regulators expect adherence to law; consumers expect valuable, trustworthy products and services; civil society expects support for the public interest. Evaluating companies according to certain standards and comparing their performance can incentivize competition among companies. It can also provide valuable information to various stakeholders, who can likewise pressure companies to perform better. The Ranking Digital Rights project (RDR) developed criteria to evaluate companies in the information and communications technology (ICT) sector on their respect for free expression and privacy rights[1] (Maréchal, 2015).

RDR's criteria, which stem from nearly four years of consultation and testing, build on several existing human rights frameworks and principles and translate them into concrete, measurable indicators. While imperfect, this approach provides a mechanism to evaluate and compare companies (Maréchal, 2015). RDR's privacy indicators draw from the Fair Information Practice Principles, OECD Privacy Guidelines, European Union regulations, and other frameworks (Ranking Digital Rights, 2016a). The indicators related to company data practices focus on company disclosure related to the collection, sharing, use, and retention of user information as well as users' ability to access and control their own information (Ranking Digital Rights, 2016b). Often, company disclosure about these practices appears in a privacy policy.

Policy documents alone cannot reveal whether companies respect privacy rights, but they do represent company practice. Privacy policies notify the public, and regulators in particular, about a company's privacy practices. As such, they serve as an important source of information to understand how users' privacy rights fare online. Scholars, journalists, and those in civil society have studied privacy policies for this purpose, and some privacy policy research has taken a longitudinal approach (Jeong, 2016; Milne, Culnan, & Greene, 2006; Opsahl, 2010). In this paper, I draw on my experience studying privacy policies for RDR to evaluate how changes in the PRISM company privacy policies suggest shifts in users' privacy rights. I particularly focus on changes related to the life cycle of user information.

3. Locating and Analyzing Company Privacy Policies

This study compares versions of ten privacy policies in effect before and after two points in time:

1. The date the company entered PRISM, according to documents from Snowden (Gellman & Poitras, 2013). These dates range from September 2007 to October 2012.
2. June 6, 2013, the day the Washington Post published its story on PRISM, alerting the public to the program's existence (Gellman & Poitras, 2013).[2]

It includes the nine companies implicated in PRISM as well as Twitter, which attracted media attention for its absence from the list of PRISM companies (Martin, 2013). Since Twitter was not publicly named as a PRISM company, I only analyzed it for the second time frame.

Google and Twitter provide archives of their privacy policies. For the remaining companies, I used the Internet Archive's Wayback Machine to find previous versions of their privacy policies. Murphy, Hashim and O'Connor (2007) suggest the Wayback Machine is a valid source when examining website content and age. To check the Wayback Machine's validity for this study, I compared versions of Google and Twitter's policies from their company archives and the Wayback Machine. The text was identical in both versions, except the Wayback Machine version of one policy lacked a reference to Google's archive. This suggests the Wayback Machine provides adequate representations of previous versions of privacy policies.

Table 1 lists the policies used for each company. All companies except Paltalk included the date the policy was last updated or the date the policy went into effect, which made it easy to determine when the policies changed. The first time frame includes three policies for Paltalk because the first updated policy only contained a change in the company's mailing address. Paltalk's second updated version included one substantive change. Corporate oversight structures also influenced which policies were reviewed. Google has owned YouTube since 2006. During the first time frame, YouTube maintained a separate privacy policy, so changes in its policies are included in this analysis. By the second time frame, Google's privacy policy covered all of its services, including YouTube, so that period does not include an analysis of separate YouTube policies. Conversely, Microsoft bought Skype in 2011, but Skype maintained a separate privacy policy during both time frames and is included in both.

I used a difference-checking tool to identify the changes in each company's "before" and "after" policies. I logged each change in a spreadsheet. The addition or removal of an entire sentence represented one change. If one sentence included several distinct edits, I logged them separately. I looked at the original policies to determine whether the change was substantive, using an inductive approach to develop codes related to the substance of changes (Thomas, 2006). In the first pass, I developed the codes and assigned them to each change. I took a second pass through the entire dataset and checked for consistency. Table 2 contains examples of each code. These codes were mutually exclusive.

Overall, the policies included 814 changes, with Facebook accounting for 651, or 80 percent. Facebook overhauled its policy during the first time frame and made significant changes during the second time frame, far outpacing the number of changes from other companies. In

[1] Until August 2016, I was a research analyst with the RDR project.

[2] The Washington Post first reported the story on June 6, 2013 and updated its story on June 7, 2013 (Blodget, 2013).

Table 1. Privacy policies analyzed across two time frames.

Company	Date of Policy	Timeframe 1: Entered PRISM	Date of Policy	Date of Policy	Timeframe 2: PRISM News	Date of Policy
Microsoft	Jan. 2006	Sept. 11, 2007	Oct. 2007	April 2012	June 6, 2013	Aug. 2013
Yahoo	Nov. 22, 2006	Mar. 12, 2008	Oct. 28, 2008	May 31, 2013		Sept. 25, 2014
Google	Aug. 7, 2008	Jan. 14, 2009	Jan. 27, 2009	July 27, 2012		June 24, 2013
Facebook	Nov. 26, 2008	June 3, 2009	Nov. 19, 2009	Dec. 11, 2012		Nov. 15, 2013
Paltalk	Oct. 7, 2009 (crawled)	Dec. 7, 2009	Feb. 7, 2010; Dec. 4, 2010 (crawled)	May 19, 2013		No change
YouTube	Mar. 11, 2009	Sept. 24, 2010	Dec. 8, 2010	See Google		See Google
Skype	Nov. 2010	Feb. 6, 2011	June 2011	Dec. 2012		Aug. 2013
AOL	Feb. 14, 2011	Mar. 31, 2011	Mar. 30, 2012	May 14, 2013		June 28, 2013
Apple	May 21, 2012	Oct. 2012	No change	No change		Aug. 1, 2013
Twitter	N/A	N/A	N/A	May 17, 2012		July 3, 2013

Table 2. Examples of substantive and non-substantive changes in privacy policies.

Substantive Changes	Explanation or Example
Addition of information	Added sentence: "When we display personalized ads, we take a number of steps designed to protect your privacy."
Removal of information	Removed sentence: "You will only receive special offers via email from Paltalk if you have indicated in your account preferences, or at some other time, that you would like to receive them."
More precise information	Added the bold phrase: "If we learn that we have collected the personal information of a child under 13 **without first receiving verifiable parental consent** we will take steps to delete the information as soon as possible."
Less precise information	Changed the bolded phrase from: "If you are under 13, please do not attempt to register for Facebook or **send any information about yourself to us, including your name, address, telephone number, or email address**" to "If you are under age 13, please do not attempt to register for Facebook or **provide any personal information about yourself to us.**"
Non-Substantive Changes	
Simple fact change	Changed the "Last updated" date in a policy.
Position change	Moved a sentence from one paragraph in the policy to another.
Style change	Changed phrase from: "**NOTICE: Click here for practical tips from the federal government and the technology industry** to help you guard against Internet fraud, secure your computer and protect your personal information" to "**The federal government and technology industry have developed practical tips** to help you guard against Internet fraud, secure your computer and protect your personal information" [Hyperlink present in both sentences].
Fixing typos	Changed phrase from: "To protect your privacy and **security, may** use passwords to help verify your identity before granting access or making corrections to your AOL information" to "To protect your privacy and **security, we may** use passwords to help verify your identity before granting access or making corrections to your AOL information."

total, the policies showed 424 substantive changes, with Facebook accounting for 347, or 82 percent. This analysis focuses on the substantive changes. To answer the question of what these policy changes suggest with regard to the life cycle of user information, I again used an inductive approach to develop codes related to digital rights, as framed by RDR's indicators (Ranking Digital Rights, 2016b; Thomas, 2006). In a first pass, I developed and assigned the codes to each substantive change and in a second pass, I checked for consistency. This yielded 11 codes across four themes. These codes were not mutually exclusive, and 30 changes received two codes (25 of those changes applied to Facebook). Table 3 shows the themes and the codes present in each. It also states how many changes related to each theme appeared in Facebook's policies compared to other companies.

Table 3. Digital rights themes and codes.

Digital Rights Theme	Codes Included in Theme	Number of Changes (Not Mutually Exclusive)
Management of user information	Data collection, Use of data, Retention, Security	146 (Facebook: 133)
Data sharing and tracking	Third party, Data sharing, Tracking	149 (Facebook: 115)
User action	More information, Choice	115 (Facebook: 89)
Corporate governance	Accountability, Remedy	44 (Facebook: 35)

4. Policy Changes Related to the Life Cycle of User Information

Two of the four digital rights themes focused on the life cycle of user information: management of user information and data sharing and tracking. Together, these themes encompassed 70 percent of the substantive changes. The following analysis describes what the changes suggest for users' privacy.

4.1. Management of User Information

Over both time frames, Facebook's policies in particular included many changes related to the company's collection and use of information. Positively, changes during the first time frame clarified what information the company requires when new users join, and what additional information users can provide. The revised policy contained clear examples of what Facebook considers user content; the previous version of the policy told users to check the company's Terms of Use for a definition. However, the policy changes also disclose Facebook collecting more user information over both timeframes (see Annex Table A.1., rows 1–2, changes in bold).

Microsoft and Facebook included changes related to retention. In the first time frame, Microsoft positively added a sentence stating that it stores information about a user's behavior (e.g. page views, clicks, and search terms) separately from information that identifies the user (e.g., name, e-mail address) (see Table A.1., row 3). Somewhat positively, Facebook added a sentence describing a time frame in which it anonymizes data it receives from advertisers, but it applies only to information the company doesn't already have (see Table A.1., row 4). This suggests that some advertising-related user information is not subject to anonymization. In the second time frame, Facebook stated that apps connected to Facebook might retain user information after users delete the app (see Table A.1., row 5). Facebook also added a sentence saying users could contact the app directly and request deletion of their data.

Overall, changes across both timeframes suggest companies, primarily Facebook, provided additional detail regarding what they collect and how they manage it. In some cases, this can help users better understand company practices, for example what information they must provide and what is optional.

4.2. Data Sharing and Tracking

Yahoo and Facebook included changes related to sharing user information with governments, though the changes do not appear to be linked to PRISM (see Annex Table A.2., rows 1–2). Yahoo stated that it responds to law enforcement requests; PRISM requests fall under national security. Facebook added a sentence stating that it may disclose user information in response to requests from foreign jurisdictions; PRISM requests come from the U.S. government.

Several companies added information to policies related to their use of targeted advertising: Microsoft and YouTube in the first time frame; Skype, Yahoo, and Twitter in the second time frame; and Facebook across both timeframes. Changes in Facebook's policies appeared to give the company wider latitude in sharing user information, particularly with advertisers.

In the first time frame, Microsoft added more companies as advertising partners. It also listed the types of data it uses to target advertising (see Table A.2., row 3). Microsoft added that advertising networks compile information "over time" about where users click or see advertisements and may "associate this information with your subsequent visit, purchase or other activity on participating advertisers' websites in order to determine the effectiveness of the advertisements". Finally, Microsoft removed a sentence from its policy, raising questions about its access to advertising networks' cookies (see Table A.2., row 4). Changes in YouTube's policies state that it shows users advertising even when they are logged out, that advertisers can serve ads based on demographic categories inferred from users' behavior, and that they can serve ads based on user information obtained from other companies (see Table A.2., rows 5–7).

In the second time frame, Yahoo added two sentences to its policy that explain how it uses device identifiers to target advertising, framed in the parlance of personalization (see Table A.2., row 8). Twitter added two sentences about user information it may receive from advertising partners (see Table A.2., row 9). Skype added language suggesting that third-party advertisements would appear on its various sites and that Skype and its advertising partners would receive information (changes in bold) "about your relationship with **and use of** Skype's websites, software, and products…".

Changes in Facebook's policies over both time frames appeared to give the company wider latitude to share information, particularly with advertisers. In the first time frame, Facebook removed the phrase stating that it shares information with third parties "only in limited circumstances". The policy gained two sentences explaining what types of information Facebook uses when targeting advertising and how advertisers may interact with users. Facebook stated it only uses non-personally identifiable attributes but then stated that it may use sensitive, personal information to target advertising, and that advertisers may be able to discern that information (see Table A.2., row 10). In the second time frame, Facebook revised the following sentence about how it shares information with advertisers (changes in bold):

> 2012: We only provide data to our advertising partners or customers after we have removed your name or any other personally identifying information from it, or have combined it with other people's data in a way that it is no longer **associated** with you.
>
> 2013: We only provide data to our advertising partners or customers after we have removed your name **and** any other personally identifying information from it, or have combined it with other people's data in a way that it no longer **personally identifies** you.

While the shift from "or" to "and" seems to provide greater protection to users, the shift from the higher threshold of association to the lower threshold of "personally identifiable" seems to negate that protection, because information that does not personally identify a user can still be associated with a user and thus can identify the user. Facebook also revised its policy to more clearly state that it uses all user information to target advertising (see Table A.2., row 11).

While these additions provide more detail for users to understand company practices, the practices themselves appear to subject users to greater tracking for advertising purposes. They include examples of companies tracking users in more circumstances and using more information to target those ads. The disclosures also use jargon such as "non-personally identifiable information" and "device identifiers" and they reference the data processing techniques of inference and association, the nuances of which are likely unfamiliar to average users. This can make it difficult for anyone who actually reads privacy policies to fully understand what the policies mean.

5. Privacy Policy Changes Offer Evidence of Surveillance Capitalism

Collectively, these privacy policy changes offer evidence that suggests several of the world's largest Internet companies operate according to the logic surveillance capitalism. We cannot know whether these privacy policy changes reflected actual changes in company practice or if they provided more detail about practices in which companies already engaged. But the changes suggest that between the time the companies joined PRISM and the public learned of PRISM, companies disclosed that they managed more user information and, in particular, broadened their targeted advertising.

Targeted advertising is the dominant business model that powers most Internet companies today (Richards, 2013). This entails collecting data from individuals' digital interactions, however minor: "Facebook 'likes', Google searches, emails, texts, photos, songs, and videos, location, communication patterns, networks, purchases, movements, every click, misspelled word, page view, and more" (Zuboff, 2015, p. 79). Companies then employ advanced data analysis techniques to determine how to use such data to extract revenue from advertisers, transforming the data into what Zuboff calls "surveillance assets" (2015, p. 80).

As a condition for using such services, people must agree to terms such as those in privacy policies, whose narrow definitions and vague language prevent people from understanding how their data flows through the life cycle of user information (Kumar, 2016). This model, which puts the onus on users to manage their own privacy and hinges on whether they "consent" to such practices, does not meaningfully protect users' privacy (Solove, 2013).

Beyond disclosing their practices in policies, companies justify their big data activities by arguing that users gain something in return, for example, free services or personalized experiences. People pay for these benefits by foregoing their right to decide whether to disclose a given facto or keep it to themselves. As such, surveillance does not erode privacy rights; it redistributes them, enabling companies or governments to know information about people without their ever having a choice (Reidenberg, 2015; Zuboff, 2015).

PRISM is one example of "the blurring of public and private boundaries in surveillance activities...between state security authorities and high tech firms" (Zuboff, 2015, p. 86). Companies collect and retain massive amounts of data about their users—itself an act of surveillance (Richards, 2013)—and the NSA can compel companies to turn over that data for targeted surveillance. The PCLOB report (2014) reviewed the checks and balances under which the government's PRISM program operates. However, the surveillance activities of companies in PRISM do not operate with as much oversight. Debates about privacy rights in a post-Snowden world cannot ignore the fact that companies have business incentives to collect and retain the data that governments can obtain through surveillance activities.

6. Conclusion: Government Surveillance as a Symptom of Surveillance Capitalism

PRISM did not cause surveillance capitalism, but this analysis suggests that PRISM companies further en-

meshed themselves in it over the past decade. They did so while belonging to a secret surveillance program in which the U.S. government could compel them to turn over all the information they had associated with a given user's email address or telephone number. The PRISM companies serve billions of users worldwide. They have the power to adopt business practices that significantly enhance the privacy of everyday users. This analysis of privacy policy changes that companies made between joining PRISM and PRISM's disclosure to the public suggests that companies went in the other direction by expanding their use of targeted advertising. It illustrates that public debates about people's privacy rights in the wake of the Snowden disclosures must not ignore the role that companies themselves play in legitimizing surveillance activities under the auspices of creating market value.

Acknowledgements

I thank Nathalie Maréchal, Katie Shilton, Karen Boyd, and Jessica Vitak for their input. I also thank the editors and three anonymous reviewers, whose feedback significantly strengthened this work.

Conflict of Interests

The author declares no conflict of interests.

References

Bellia, P. L. (2008). The memory gap in surveillance law. *University of Chicago Law Review*, *75*, 137–179.

Blodget, H. (2013, June 7). The Washington Post has now hedged its stunning claim about Google, Facebook, etc, giving the government direct access to their servers. *Business Insider*. Retrieved from http://www.businessinsider.com/washington-post-updates-spying-story-2013-6

Butler, J., & Granick, J. S. (2016). Correcting the record on section 702: A prerequisite for meaningful surveillance reform. *Just Security*. Retrieved from https://www.justsecurity.org/wp-content/uploads/2016/09/Butler-Granick-Correcting-the-Record-Scope-of-702.pdf

Gallagher, R., & Hager, N. (2016, August 14). In bungled spying operation, NSA targeted pro-democracy campaigner. *The Intercept*. Retrieved from https://theintercept.com/2016/08/14/nsa-gcsb-prism-surveillance-fullman-fiji

Gellman, B., & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. Retrieved from https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Jeong, S. (2016, January 14). The history of Twitter's rules. *Vice Motherboard*. Retrieved from http://motherboard.vice.com/read/the-history-of-twitters-rules

Kumar, P. (2016). Privacy policies and their lack of clear disclosure regarding the life cycle of user information. *2016 AAAI Fall Symposium Series*. Retrieved from http://aaai.org/ocs/index.php/FSS/FSS16/paper/view/14089

MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for Internet freedom*. New York, NY: Basic Books.

Maréchal, N. (2015). Ranking digital rights: Human rights, the Internet and the fifth estate. *International Journal of Communication*, *9*, 3440–3449.

Martin, S. (2013, June 7). Twitter notably absent from NSA PRISM list. *USA Today*. Retrieved from http://www.usatoday.com/story/tech/2013/06/07/nsa-prism-twitter/2401605

Miller, C. C. (2013, June 7). Tech companies concede to surveillance program. *The New York Times*. Retrieved from http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html

Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing*, *25*(2), 238–249. doi:10.1509/jppm.25.2.238

Murphy, J., Hashim, N. H., & O'Connor, P. (2007). Take me back: Validating the Wayback Machine. *Journal of Computer-Mediated Communication*, *13*(1), 60–75. doi:10.1111/j.1083-6101.2007.00386.x

Ni Loideain, N. (2016). The end of safe harbor: Implications for EU digital privacy and data protection law. *Journal of Internet Law*, *19*(8), 7–14.

Opsahl, K. (2010, April 28). Facebook's eroding privacy policy: A timeline. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2010/04/facebook-timeline

Privacy and Civil Liberties Oversight Board. (2014). *Report on the surveillance program operated pursuant to section 702 of the Foreign Intelligence Surveillance Act*. Washington, DC: Privacy and Civil Liberties Oversight Board.

Ranking Digital Rights. (2016a, September 14). *Methodology development*. Retrieved from https://rankingdigitalrights.org/methodology-development

Ranking Digital Rights. (2016b, September). *2017 corporate accountability index research indicators*. Retrieved from https://rankingdigitalrights.org/wp-content/uploads/2016/09/2017Indexmethodology.pdf

Reidenberg, J. R. (2015). The transparent citizen. *Loyola University Chicago Law Journal*, *47*, 437–463.

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review*, *126*, 1934–1965.

Schwartz, P. M., & Solove, D. J. (2014). Reconciling personal information in the United States and European Union. *California Law Review*, *877*, 877–916.

Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*, 1880–1903.

Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation*, *27*(2), 237–246. doi:10.1177/1098214005283748

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*, 75–89. doi:10.1057/jit.2015.5

About the Author

Priya Kumar is a doctoral student at the University of Maryland College of Information Studies. She studies privacy from various perspectives, including corporate accountability and computer-mediated communication. Priya holds an MS in Information from the University of Michigan and BA degrees in journalism and government and politics from the University of Maryland. Find her on Twitter at @DearPriya.

Annex

Table A.1. Privacy policy changes related to management of user information.

	Company	Timeframe 1		Timeframe 2	
		Pre-Join PRISM	Post-Join PRISM	Pre-PRISM Disclosed	Post-PRISM Disclosed
1	Facebook	2008: "When you enter Facebook, we collect your browser type and IP address."	2009: "When you **access** Facebook **from a computer, mobile phone, or other device**, we **may** collect **information from that device about** your browser type, **location**, and IP address, **as well as the pages you visit**."		
2	Facebook			2012: "This may include your IP address and other information about things like your Internet service, location, the type (including identifiers) of browser you use, or the pages you visit."	2013: "This may include **network and communication information, such as** your IP address **or mobile phone number**, and other information about things like your Internet service, **operating system**, location, the type (including identifiers) **of the device or** browser you use, or the pages you visit."
3	Microsoft		2007: **Added** "For example, we store page views, clicks and search terms used for ad personalization separately from your contact information or other data that directly identifies you (such as your name, e-mail address, etc.)."		
4	Facebook		2009: **Added** "If in any of these cases we receive data [from advertising partners] that we do not already have, we will 'anonymize' it within 180 days, meaning we will stop associating the information with any particular user."		
5	Facebook				2013: **Added** that when users delete an app connected to Facebook, "it [the app] may still hold the information you have already shared."

Table A.2. Privacy policy changes related to data sharing and tracking.

	Company	Timeframe 1		Timeframe 2	
		Pre-Join PRISM	Post-Join PRISM	Pre-PRISM Disclosed	Post-PRISM Disclosed
1	Yahoo			2013: "We respond to subpoenas, court orders, or legal process or to establish or exercise our legal rights or defend against legal claims."	2014: "We respond to subpoenas, court orders, or legal process **(such as law enforcement requests)**, or to establish or exercise our legal rights or defend against legal claims."
2	Facebook	2008: "We may **be required to** disclose user information pursuant **to lawful requests, such as subpoenas or court orders**, or in compliance with applicable laws. **We do not reveal information until** we have a good faith belief that **an information request by law enforcement or private litigants meets applicable legal standards**."	2009: "We may disclose information pursuant to **subpoenas, court orders, or other requests (including criminal and civil matters)** if we have a good faith belief that **the response is required by law. This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards.**"		
3	Microsoft		2007: **Added** "For example, we may select the ads we display according to certain general interest categories or segments that we have inferred based on "(a) demographic data, including any you may have provided when creating an account (e.g. age, zip or postal code, gender), general demographic data acquired from other companies, and a general geographic location derived from your IP address, (b) the pages you view and links you click when using Microsoft's and its partners' web sites and		

Table A.2. Privacy policy changes related to data sharing and tracking. (Cont.)

	Company	Timeframe 1		Timeframe 2	
		Pre-Join PRISM	Post-Join PRISM	Pre-PRISM Disclosed	Post-PRISM Disclosed
3	Microsoft		services, and (c) the search terms you enter when using Microsoft's Internet search services, such as Live Search."		
4	Microsoft		2007: **Removed** "Microsoft does not have access to the cookies that may be placed by the third-party ad servers or ad networks."		
5	YouTube	2009: "**If** you are **logged into** your YouTube Account, we may also show you advertising based on **the information** you have provided to us in your YouTube Account."	2010: "**While** you are logged in **or logged out** of your YouTube Account, we may also show you advertising based on **non personally identifiable** information you have provided to us in your YouTube Account."		
6	YouTube	2009: "Advertisers may serve ads based on **interests** associated with non-personally identifiable online activity, such as videos viewed, frequency of uploading or activity on other AdSense partner sites."	2010: "Advertisers may serve ads based on interests **and demographic categories** associated with non-personally identifiable online activity, such as videos viewed, frequency of uploading or activity on other AdSense partner sites."		
7	YouTube	2009: "Advertisers may also serve ads to you based on previous activity on that advertiser's website."	2010: "Advertisers may also serve ads to you based on previous activity on that advertiser's website **or based on non-personally identifiable information from other companies**."		
8	Yahoo				2014: **Added** "We may also set and access device identifiers which could include IP address, user agent information (browser version, OS type and version), and device provided identifiers. Once you log into Yahoo on your device, Yahoo may recognize your device to provide you with a

Table A.2. Privacy policy changes related to data sharing and tracking. (Cont.)

	Company	Timeframe 1		Timeframe 2	
		Pre-Join PRISM	Post-Join PRISM	Pre-PRISM Disclosed	Post-PRISM Disclosed
8	Yahoo				personalized experience, independent of your device settings."
9	Twitter				2013: **Added** "Third-party ad partners may share information with us, like a browser cookie ID or cryptographic hash of a common account identifier (such as an email address), to help us measure ad quality and tailor ads. For example, this allows us to display ads about things you may have already shown interest in."
10	Facebook		2009: **Added** "We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected (including information you may have decided not to show to other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements...Even though we do not share your information with advertisers without your consent, when you click on or otherwise interact with an advertisement there is a possibility that the advertiser may place a cookie in your browser and note that it meets the criteria they selected."		

Table A.2. Privacy policy changes related to data sharing and tracking. (Cont.)

	Company	Timeframe 1		Timeframe 2	
		Pre-Join PRISM	Post-Join PRISM	Pre-PRISM Disclosed	Post-PRISM Disclosed
11	Facebook			2012: "We use the information we receive, including the **information you provide at registration or add to your account or timeline, to deliver** ads **and to make them** more relevant to you."	2013: "**So we can show you content that you may find interesting**, we **may** use all of the information we receive **about you** to serve ads that are more relevant to you."