International Journal of Communication 9(2015), Feature 3450–3459 1932–8036/2015FEA0002

IJoC Communication in Action

Surveillance of Communications: A Legitimization Crisis and the Need for Transparency

JAMES LOSEY[1]
Stockholm University, Sweden

Keywords: surveillance, transparency, policy, legitimacy, Habermas transparency reporting

Introduction

The surveillance of communications faces a legitimization crisis. The information and communication technologies (ICT) that facilitate contemporary communications, from mobile phones to social media platforms, can also facilitate surveillance. The position of ICT services in mediating communications places companies in a position to be under legal and extralegal pressure from law enforcement and other government agencies turn over details of user communications as well as remove content. The collection of communications data by governments has increased precipitously in recent years, in part due to changing technologies. As Bankston and Soltani (2014) document, surveillance historically required considerable costs and manpower. For example, where tracking the location of an individual might have involved multiple police officers in the past, today this data is often collected by telecommunications companies and then accessed by law enforcement on request, lowering the costs of bulk surveillance (ibid.).

Surveillance is a global concern, and the security agencies of democratic states leverage the data from ICT companies and services to conduct bulk surveillance. Examples include the collection of interstate Internet traffic by the Försvarets Radioanstalt (FRA) in Sweden, or the global surveillance reach of the National Security Administration (NSA) in the United States. For example, the NSA found mechanisms to access data transferred between Yahoo and Google's data centers without the companies' knowledge (Gellman & Soltani, 2013). Law enforcement agencies also request user data from companies through extralegal or informal processes.

[1] The author acknowledges and thanks Susan Morgan, David Sullivan, Lisl Brunner, and the Global Network Initiative for the opportunity to be a Google Policy Fellow during 2014, which helped inform this research, and Victor Pickard, Mark Lloyd, and Jason Smith for the opportunity to participate in the COMPASS fellows program and contribute to this issue. Helpful critique from anonymous reviewers contributed to this article.

The legitimization crisis of the current surveillance practices stems from both the scope and the shortcomings of accountability. The full extent of the different programs is unknown, limiting the ability for democratic society to evaluate current practices on rational grounds. At the same time, the extent that bulk surveillance takes place violates the right to privacy. In June 2014, Navi Pillay, the United Nations High Commissioner for Human Rights, criticized the practice in a report to the United Nations, writing that "In other words, it will not be enough that the measures are targeted to find certain needles in a haystack," but the potential harms must be considered to evaluate whether surveillance is "necessary and proportionate" (Pillay, 2014, p. 9).

Transparency is a critical step toward accountability of the mechanisms through which law enforcement and government agencies access communications data. Since 2010, a growing contingent of ICT companies have begun to publish transparency reports on the extent that governments request their user data, and some include requirements to remove content as well. However, governments have fallen short on providing the level of detail on surveillance programs that is necessary for informed debate. The importance of transparency for the removal of content from online platforms is also addressed, though the focus is on surveillance. This article offers an overview of transparency reports currently published by ICT companies and discusses why increased transparency is a necessary but insufficient condition for accountability and supporting democratic debates on the practice and extent of surveillance of communications. Furthermore, this article discusses why governments are well-positioned to provide a greater level of transparency on the legal processes and technical means through which law enforcement actors and agencies access private communications data.

Transparency and Legitimacy

The collection of communications data from users of ICT services takes place under different legal processes in different countries. Practices include court-ordered requests of data from ICT companies, such as accessing the emails of a suspect during an investigation. However, data collection often takes place without due process or under nonpublic legal justifications. For example, in Sweden, all cross-border Internet traffic is shared with the FRA, and the FRA later filters the data to focus on a specific search (Klamberg, 2010). In the United States, bulk collection of telephony data takes place under section 215 of the USA Patriot Act following secret court rulings in 2004 and 2006 by the Foreign Intelligence Surveillance Act (FISA) Court (Geiger, 2014; Savage & Poitras, 2014). In 2007, the FISA court authorized warrantless wiretapping of international phone calls and emails (Savage & Poitras, 2014). The NSA also exploited or actively created security holes to gain access to communications data (Glanz, Larson, & Lehren, 2014; Mehn, 2013). The Global Communications Headquarters in the UK taps fiberoptic cables to share international traffic with the NSA, including phone calls, email messages, and social media entries (MacAskill, Borger, Hopkins, Davis, & Ball, 2013).

In addition to the human rights concerns raised by bulk surveillance, the lack of transparency of these programs creates a legitimization crisis. Jürgen Habermas presents a theory of legitimization dependent on three conditions: a normative order, that order is established on rational grounds, and that an order has the support of the subjects (Habermas, 1975, p. 98). Without these conditions, a state or policy loses legitimacy. Habermas cautions that pure legality "will not be able to guarantee recognition in

the long run if the system of authority cannot be legitimized independently of the legal form of exercising authority" (ibid., p. 100). A purely legal structure can be exemplified by an authoritarian framework featuring top-down power lacking in populist support. Furthermore, Cohen writes that "democratic politics involves public deliberation focused on the common good, requires some form of manifest equality among citizens, and shapes the identity and interests of citizens in ways that contribute to the formation of public conception of common good" (2002, p. 344). In order for governments to support the public deliberation on rational grounds about the collection of surveillance, details on the scope and processes of surveillance programs must be revealed. Reporting the extent that communications data is restricted, monitored, or collected provides a critical window into the scope of contemporary surveillance and censorship. In the most recent annual report of the interception of communications, the UK Commissioner Sir Anthony May writes that "the unreliability and inadequacy of the statistical requirements is a significant problem which requires attention" (2013, p. 24), and a problem that transparency reporting can address.

Transparency reporting mechanisms are a vital component for debating the efficacy and validity of content censorship and lawful interception of communications in an open society. Several companies publish some details, and the reports published thus far have begun to provide a foundation of data for analysis. However, the currently available details are insufficient in countries such as the United States, Sweden, the UK, and countless others.

Companies and Reporting

ICT companies are in a position to provide transparency on the extent that content is removed or data is provided to law enforcement in the countries in which they operate, and some have been leading the vanguard. Google first launched their transparency report in September 2010 (Schroeder, 2010). In her book *Consent of the Networked*, Rebecca MacKinnon noted that Google's goal was to "start a conversation about censorship and surveillance" (2012, p. 245). Google has continued to publish semiannual reports, and the initiative for transparency was soon followed by Twitter, Dropbox, Microsoft, and others. Today, more than 40 companies in the ICT sector publish transparency reports (See Table 1). Some companies publish numbers for multiple countries, such as Google (101 countries), Facebook (71 countries), Microsoft (66 countries), Twitter (54 countries), Vodafone (29 countries), and Yahoo (39 countries) (Losey, 2015). Currently, transparency reports from ICT companies vary in what they report. For example, few transparency reports include the amount of content that is removed for copyright reasons (though CyberGhost, Facebook, Google, and Twitter do). Additionally, most transparency reports do not include details on whether content has been removed due to government requests (Facebook, Google, Twitter, Verizon, Wikimedia, and Wordpress are examples of companies that do report this). In the event that content is blocked in a specific country, Twitter shares the original removal request with Chilling Effects Clearinghouse (Twitter, 2012), a website that also publishes Digital Millennium Copyright Act takedown requests. Like reporting on law enforcement access to user data, reporting the extent that governments require content to be restricted helps to document the extent that intermediary liability laws hinder freedom of expression. Reporting the extent to which content is restricted is one area of improvement for the ICT sector with regards to transparency reporting.

Table 1. Overview of Transparency Reports.

	Countries/Regions	User Data	National Security	Content Restriction	Copyright
AOL	U.S.	Yes	Yes	No	No
Apple	63 Countries	Yes	(U.S.)	No	No
AT&T	U.S.	Yes	Yes	No	No
Cloudflare	U.S.	Yes	Yes	No	No
Comcast	U.S.	Yes	Yes	No	No
Credo	U.S.	Yes	Yes	No	No
CyberGhost	21 Countries	Yes	No	No	Yes
Deutsche Telekom	Germany	Yes	No	No	No
DaumKakao	South Korea	Yes	No	No	No
Dropbox	U.S.	Yes	Yes	No	No
Evernote	U.S.	Yes	Yes	No	No
Facebook	71 Countries	Yes	(U.S.)	Yes	Yes
Google	101 Countries	Yes	(U.S.)	Yes	(Search)
Internet Archive	U.S.	Yes	Yes	No	No
LeaseWeb	3 Countries	Yes	No	Yes	No
LinkedIn	11 countries	Yes	(U.S.)	No	No
Lookout	U.S./Germany	Yes	US	No	No
Mapbox	Global	Yes	No	Yes	Yes
Medium	U.S.	Yes	Yes	Yes	Yes
Microsoft	69 Countries	Yes	(U.S.)	No	No
Pinterest	U.S.	Yes	Yes	No	No
Posteo	Germany	Yes	No	No	No
Reddit	U.S. / Other	Yes	Yes	Yes	Yes
Rogers	Canada	Yes	No	No	No
SaskTel	Canada	Yes	No	No	No
Silent Circle	U.S.	Yes	No	No	No
Sonic.net	U.S.	Yes	No	No	No
SpiderOak	U.S.	Yes	No	No	No
TekSavvy	Canada	Yes	No	No	No
TeliaSonera	7 Countries	Yes	Yes[2]	No	No
Telstra	Australia	Yes	No	No	No
Telus	Canada	Yes	No	No	No
Time Warner Cable	U.S.	Yes	Yes	No	No
Tumblr	12 Countries	Yes	(U.S.)	No	No
Twitter	54 Countries	Yes	(U.S.)	Yes	Yes
Verizon	16 Countries	Yes	(U.S.)	Yes	No

[2] National security and secret police requests are aggregated with law enforcement requests for Denmark, Estonia, Finland, Nepal Norway and Spain. In Sweden, TeliaSonera receives secret police requests via police (TeliaSonera, 2015).

Vodafone	28 Countries	Yes	Unclear	No	No
Wickr	U.S. and Other	Yes	No	No	No
Wikimedia	38 Countries	Yes	No	Yes	Yes
Wind Mobile	Canada	Yes	No	No	No
Wordpress	24 Countries	Yes	(U.S.)	Yes	Yes
Yahoo	39 Countries	Yes	Yes	Yes	No

Transparency reports provide a window into the extent that law enforcement agencies request access to user data. For example, during the first six months of 2014, Twitter received 1,257 requests for user data from the U.S. government. These requests affected 1,918 accounts, and Twitter complied with 72% of them. During the same period, Google received 12,539 requests from the U.S. government, up from 10,574 in the previous six-month period. These requests affected 21,576 accounts, and Google and complied with 84% of them. By comparison, Germany made 3,338 requests to Google for user data from 4,272 accounts (some data was produced for 48% of these requests) and 14 requests to Twitter for 28 accounts (some data was produced for 21% of cases). From January to June 2014, Facebook received 15,433 requests from U.S. law enforcement for information from 23,667 users and produced at least some data in response to 80% of the requests, and also received 2,537 requests from law enforcement in Germany affecting 3,078 users and produced at least some data in 34% of those cases.

Reporting the extent to which governments request access to user data is critical for understanding the pressures placed on companies to participate in government surveillance, as well as the extent to which these companies cooperate. In their reports, the companies report the number of requests, but vary in the details. For example, while Facebook, Google, and Twitter report cases where some data is produced, Microsoft, Tumblr, and Yahoo distinguish between cases where content (such as messages) is produced versus non-content (such as a user's contact information). Additionally, when analyzing transparency reports for requests outside of the United States, reports rarely document the legal processes through which law enforcement requests for data are made. In fact, when comparing Facebook, Google, LinkedIn, Microsoft, Tumblr, Twitter, Verizon, and Yahoo, it became clear that none of the companies reported legal processes used for request for users data from non-U.S. governments.

However, while some of the gaps in transparency reports result from the ways that companies compile and report numbers, another gap results from types of requests that are restricted from being reported. Not all companies report aggregate numbers for national security requests. For example, different laws under which the U.S. government can access user data include three statutes of the Electronic Communications Privacy Act (ECPA): the Stored Communications Act, the Wiretap Act, and the Pen Register Statute. Additional statutes include National Security Letters and the FISA court. An analysis from the New America Foundation reviewing transparency reports noted that only Google and Verizon differentiate between different ECPA requests in their reports, while Google also reports NSL and FISA numbers (Open Technology Institute, 2014). Vodafone's transparency report, covering 29 countries, also noted when the company was barred from reporting numbers. For example, Vodafone reported that reporting numbers related to lawful interception of communications was forbidden in Albania, Egypt, Hungary, India, Malta, the Netherlands, Romania, and South Africa (Vodafone, 2014). Additionally,

reporting numbers related to requests for communications data is unlawful in Egypt, India, South Africa, and Turkey. In the United States, some companies have begun to challenge limits on transparency. In June 2013, Microsoft, Facebook, and Google asked to be able to publish more about FISA requests, and they were granted the ability to report aggregate numbers combined with non-secret requests, which obscures the actual numbers (Franceschi-Bicchierai, 2013). In 2014, Yahoo won the ability to publish their challenge to requests from the FISA court (CDT, 2014)

How and Why Governments Should be Transparent

Governments can provide a greater level of transparency for limits on the freedom of expression and privacy than companies. Company transparency reports can illuminate the extent that any one company receives requests and how the company responds. By contrast, government transparency requests provide a much greater perspective on laws that can potentially restrict freedom of expression or impact privacy. Critically, government transparency can illustrate the full extent that requests are made across the ICT industry. Biannual or annual reporting from governments would provide a comparative data point for companies currently reporting, as well as capture how requests impact the sum of companies that might not be reporting yet, thus better illustrating the number of accounts for which data is accessed. In an analysis of government requests for user data from Internet service providers in Poland, the Panoptykon Foundation concluded that "[t]he best source of such statistics are undoubtedly government bodies and it is mainly them that should collect the information on requests directed to private entities and make it available to the general public" (Szymielewicz & Szumańska, 2014, p. 25). Indeed, a wide variety of actors calling for surveillance reforms have highlighted the need for greater transparency, including a coalition of civil society organizations calling for necessary and proportionate surveillance (Necessary and Proportionate, 2014); ICT companies such as Facebook, Google, Microsoft, Twitter, and Yahoo with the Reform Government Surveillance (2014) campaign; and Swedish Foreign Minister Carl Bildt (2013), who proposed principles for reforming surveillance. All of those encourage some level of government transparency, and the Reform Government Surveillance asks that governments "allow companies to publish the number and nature of government demands for user information." The Necessary and Proportionate coalition specifies that governments "should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities" and "at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each" (Necessary and Proportionate, 2014, para. 25).

Some countries currently report some types of data. For example, the U.S. Department of Justice publishes an annual Wiretap Report (U.S. Courts, 2013a), and the United Kingdom publishes the Interception of Communications Commissioner Annual Report (May, 2013). The 2013 U.S. report documents 3,576 interceptions authorized under state or federal jurisdictions in the United States (U.S. Courts, 2013b). These numbers present an incomplete picture of the extent of law enforcement access to communications data, as wiretaps only capture a portion of the total surveillance. Law enforcement might also request user contact or location data, numbers that are not currently reported by the U.S. government at the federal, state, or local level. For example, Verizon reports that the company received not just 1,496 wiretap orders during the 2013 in the United States, but 36,969 warrants and 164,184

subpoenas as well (Verizon, 2014). Also in the United States, AT&T received 248,343 subpoenas, 36,788 court orders, 16,685 search warrants, and 37,893 location demands during 2013 (AT&T, 2014).

The full scope of surveillance encompasses numerous law enforcement agencies operating under different jurisdictions, and company transparency reports are only able to provide a partial picture. Government agencies are positioned to provide information on how different legal justifications are used by different agencies, what type of data is collected, and the extent that data collection takes place by different agencies. Increased government reporting would support accountability on how the interpretation of specific laws is being used, and on the extent that surveillance changes between reporting periods.

Conclusion

Available transparency reports from ICT companies demonstrate the rise in government requests to obtain user communications data. However, revelations on the surveillance capabilities of the United States, Sweden, the UK, and other countries demonstrate that the available data is insufficient and falls short of supporting rational debate. Companies can contribute by increasing granularity, particularly on the legal processes through which they are required to reveal user data. However, the greatest gaps remain in the information provided directly from governments. Current understanding of the scope of surveillance can be credited to whistleblowers risking prosecution in order to publicize illegitimate government activity. The lack of transparency on government access to communications data and the legal processes used undermines the legitimacy of the practices.

Transparency alone will not eliminate barriers to freedom of expression or harm to privacy resulting from overly broad surveillance. Transparency provides a window into the scope of current practices and additional measures are needed such as oversight and mechanisms for redress in cases of unlawful surveillance. Furthermore, international data collection results in the surveillance of individuals and communities beyond the scope of a national debate. Transparency offers a necessary first step, a foundation on which to examine current practices and contribute to a debate on human security and freedom. Transparency is not the sole responsibility of any one country, and governments, in addition to companies, are well positioned to provide accurate and timely data to support critical debate on policies and laws that result in censorship and surveillance. Supporting an informed debate should be the goal of all democratic nations.

References

AT&T. (2014). AT&T's transparency report. Retrieved from http://about.att.com/content/dam/csr/PDFs/ATT_Transparency%20Report_Jan%202014.pdf

Bankston, K. S., & Soltani, A. (2014). Tiny constables and the cost of surveillance: Making cents out of *United States v. Jones*. *Yale Law Journal Online*. Retrieved from http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones

Bildt, C. (2013). Tal av utrikesminister Carl Bildt vid Seoul Conference on Cyberspace 2013, Seoul, 17 oktober, 2013. Rikesdepartmentet [Speech by Foreign Minister Carl Bildt at the Seoul Conference on Cyberspace 2013, Seoul, October, 17 2013]. Retrieved from http://www.regeringen.se/content/1/c6/22/65/90/696126a5.pdf

Cohen, J. (2002). Deliberation and democratic legitimacy. In D. Matrayers & J. Pike (Eds.), *Debates in contemporary political philosophy: An anthology* (pp. 342–360). London, UK: Routledge.

CDT. (2014, September 12). Yahoo v. U.S. prism documents. Center for Democracy and Policy. Retrieved from https://cdt.org/insight/yahoo-v-u-s-prism-documents

Franceschi-Bicchierai, L. (2013, June 11). Facebook, Microsoft join Google in government transparency request. *Mashable*. Retrieved from http://mashable.com/2013/06/11/facebook-microsoft-google-transparency

Geiger, H. (2014). Issue brief: Bulk collection of records under section 215 of the PATRIOT Act. *Center for Democracy and Technology Issue Brief*. Retrieved from https://cdt.org/blog/issue-brief-bulk-collection-of-records-under-section-215-of-the-patriot-act/

Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. Retrieved from www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Glanz, J., Larson, J., & Lehren, A. (2014, January 27). Spy agencies tap data streaming from phone apps. *The New York Times*. Retrieved from http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html

Habermas, J. (1975). *Legitimation crisis* (T. McCarthy, trans). London, UK: Heinemann.

Klamberg, M. (2010). FRA and the European convention on human rights: A paradigm shift in Swedish electronic surveillance law. Retrieved from http://www.diva-portal.org/smash/get/diva2:390333/FULLTEXT01.pdf

Losey, J. (2015). Who is publishing transparency reports? Retrieved from http://www.jameslosey.com/TransparencyReports

May, A. (2013). Annual report of the interception of communications commissioner. Retrieved from http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf

MacAskill, E., Borger, J., Hopkins, N., Davis, N., & Ball, J. (2013, June 21). GCHQ taps fiber-optic cables for secret access to world's communications. *The Guardian*. Retrieved from http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

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

Mehn, J. (2013, December 20). Exclusive: Secret contract tied NSA and security industry pioneer. *Reuters*. Retrieved from http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220

Necessary and Proportionate. (2014). International principles on the application of human rights to communications surveillance. Retrieved from https://en.necessaryandproportionate.org/

Open Technology Institute. (2014). Transparency reporting for beginners: Memo #1. Retrieved from http://oti.newamerica.net/sites/newamerica.net/files/articles/Transparency_categories_chart_022614.pdf

Pillay, N. (2014, June 30). The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights. Human Rights Council. Twenty-Seventh Session, June 30. Retrieved from http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

Reform Government Surveillance. (2014). Global government surveillance reform. Retrieved from https://www.reformgovernmentsurveillance.com

Savage, C., & Poitras, L. (2014, March 11). How a court secretly evolved, extending U.S. spies' reach. *The New York Times*. Retrieved from http://www.nytimes.com/2014/03/12/us/how-a-courts-secret-evolution-extended-spies-reach.html

Schroeder, S. (2010, September 21). Google fights censorship with transparency report. *Mashable.* Retrieved from http://mashable.com/2010/09/21/googles-transparency-report

Szymielewicz, K., & Szumańska, M. (2014). Access of public authorities to the data of Internet service users: Seven issues and several hypotheses. Panoptykon Foundation. Retrieved from http://panoptykon.org/sites/panoptykon.org/files/transparency_report_pl.pdf

TeliaSonera. (2015, January 30). "TeliaSonera Transparency Report, January 2015." Retrieved from http://www.teliasonera.com/Documents/Sustainability/transparency%20report%20jan2015/TeliaSonera%20Transparency%20Report%202015.pdf

Twitter. (2012, January 26). "The Tweets Must Still Flow." Blog Post. Retrieved from https://blog.twitter.com/2012/tweets-still-must-flow

U.S. Courts. (2013a). Wiretap report. Retrieved from http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2013.aspx

U.S. Courts. (2013b). Table 2. Retrieved from http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2013/Table2.pdf

Verizon. (2014). Verizon's transparency report for the first half of 2014. Retrieved from http://transparency.verizon.com/us-report

Vodafone. (2014). Sustainability report. Retrieved from http://www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf