EFFECTS OF GOVERNMENT SURVEILLANCE ON COMPETITION

BY ALEX MARTHEWS & CATHERINE TUCKER[1]

1 Alex Marthews is National Chair at Restore the Fourth, a nonprofit Fourth-Amendment advocacy organization. Catherine Tucker is Sloan Distinguished Professor of Management at MIT Sloan.

CPI ANTITRUST CHRONICLE DECEMBER 2022

DIGITAL PLATFORMS IMPLEMENT PRIVACY-CENTRIC POLICIES: WHAT DOES IT MEAN FOR COMPETITION?
By Reinhold Kesler

HARMING COMPETITION AND CONSUMERS UNDER THE GUISE OF PROTECTING PRIVACY: REVIEW OF EMPIRICAL EVIDENCE
By D. Daniel Sokol & Feng Zhu

EFFECTS OF GOVERNMENT SURVEILLANCE ON COMPETITION
By Alex Marthews & Catherine Tucker

POPULAR MOBILE APPS IN THE PANDEMIC ERA: A GLIMPSE AT PRIVACY AND COMPETITION
By Ginger Zhe Jin, Ziqiao Liu & Liad Wagman

PRIVACY PROTECTIONS THROUGH ANTITRUST ENFORCEMENT
By Daniel A. Hanley & Karina Montoya

HOW CAN COMPETITION POLICY AND PRIVACY PROTECTION POLICY INTERACT?
By Giuliana Galbiati & Henri Piffaut

TOWARDS DATA PORTABILITY AND INTEROPERABILITY UNDER BRAZILIAN COMPETITION LAW: CRAFTING APPROPRIATE LEGAL STANDARDS FOR ABUSE OF DOMINANCE
By Victor Oliveira Fernandes

Visit www.competitionpolicyinternational.com for access to these articles and more!

EFFECTS OF GOVERNMENT SURVEILLANCE ON COMPETITION

By Alex Marthews & Catherine Tucker

Following on from the shock of the Snowden revelations, it is now well established empirically that chilling effects from government surveillance and other privacy violations exist, that they can at least sometimes be quantified, and that significant proportions of citizens in many countries both describe themselves as being harmed by them, and alter their actual behavior in response. What is less well established or understood is how a government's interest in maintaining mass surveillance programs could affect competition. This article studies this question.

Following on from the shock of the Snowden revelations, it is now well established empirically that chilling effects from government surveillance and other privacy violations exist, that they can at least sometimes be quantified, and that significant proportions of citizens in many countries both describe themselves as being harmed by them, and alter their actual behavior in response.[2] What is less well established or understood is how a government's interest in maintaining mass surveillance programs could affect competition. This article studies this question.

I. GOVERNMENT SURVEILLANCE MAY LEAD TO A NATURAL TENDENCY TO FAVOR INCUMBENTS

History offers substantial reason to suspect that governments conducting surveillance may well actively prefer long-term, stable partnerships with incumbent firms, over an environment of small, intensely competing firms with a rapidly changing cast of senior managers. For example, the U.S. National Security Agency is reported to have developed over the years a "highly collaborative," "extraordinary, decades-long partnership" with AT&T codenamed "FAIRVIEW," and a further partnership with Verizon and MCI codenamed "STORMBREW," to surveil Internet traffic passing through their servers.[3]

Early literature on the topic of the interaction between surveillance concerns and antitrust speculates about an opposite concern: That expanding government surveillance powers might enable the government to surveil firms, uncover evidence of anti-competitive practices, and result in more severe antitrust enforcement.[4] This does not seem to have occurred, perhaps because courts have construed narrowly the PATRIOT Act's expansion of DOJ wiretapping powers in the area of antitrust investigations.

However, there is evidence in that the fears expressed in this article may have come true on occasions. In litigation documents reported on in 2007,[5] for example, the former CEO of Qwest, an AT&T and Verizon competitor, alleged that the U.S. government withdrew promised contracts as retaliation for Qwest's refusal to cooperate with unlawful surveillance requests in February 2001, placing Qwest at a competitive disadvantage. The telecommunications companies' cooperation with government surveillance programs has been the subject of considerable litigation from 2006 through to 2022.[6] If these allegations were true, then, the U.S. government acted to limit the set of telecommunications providers serving U.S. customers to the set of firms who had agreed to cooperate with illegal executive branch surveillance of their users.

Another example is given by the fact that in 2014, Lavabit was a small email provider that marketed itself as providing particularly private and heavily encrypted email services, with a premium offering that offered the highest level of encryption.[7] This attracted Edward Snowden to sign up to their service. After he came forward, the FBI approached Lavabit's CEO, Ladar Levison, with a 'pen register' order for the metadata for Snowden's account. Levison explained that the account-level encryption Snowden had paid for made it impossible for Lavabit to read the metadata on his email. The FBI then ordered him to disclose his "developer-level keys," decrypting all Lavabit accounts so that they could reach Snowden's. Eventually, Levison provided the keys in a form the FBI could easily read, but chose to shut down his service the next day, rendering those keys useless, rather than to "become complicit in crimes against the American people." Again, taken by the executive branch of the U.S. government - that had the effect of limiting the options available to U.S. consumers, to offerings that enabled law enforcement decryption of content.

---

2 See Marthews, A. & Tucker, C. E., "Government surveillance and internet search behavior. SSRN." (2014); Marthews, A. & Tucker, C. E., The Impact of Online Surveillance on Behavior (June 18, 2017). Cambridge Handbook of Surveillance Law, available at SSRN: https://ssrn.com/abstract=3167473; Marthews, A., & Tucker, C. E., "Privacy policy and competition." Brookings Paper (2019); Penney, J. W. (2016), "Chilling effects: Online surveillance and Wikipedia use," Berkeley Technology Law Journal 31, 117; Penney, J. W. (2017), "Internet surveillance, regulation, and chilling effects online: A comparative case study," Internet Policy Review; Stoycheff, E. (2016), "Under surveillance: examining Facebook's spiral of silence; effects in the wake of NSA internet monitoring," Journalism & Mass Communication Quarterly 93(2), 296–311.

3 See Angwin, J., Larson, J., Moltke, H., Poitras, L., Risen, J. & Savage, C., "AT&T Helped U.S. Spy on Internet on a Vast Scale," *New York Times*, August 15, 2015, available at https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html, accessed December 7, 2022.

4 See Donald, E. S., *Electronic Surveillance and Antitrust Investigations: The Effect of the Reauthorized Patriot Act*, 41 U.C. Davis L. Rev. 387 (2007).

5 See Eggen, D. & Nakashima, E., "Former CEO Says U.S. Punished Phone Firm," available at https://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202485.html, accessed December 7, 2022.

6 For an overview, see Cohn, C., "EFF's Flagship Jewel v. NSA Dragnet Spying Case Rejected by the Supreme Court," June 13, 2022, available at https://www.eff.org/deeplinks/2022/06/effs-flagship-jewel-v-nsa-dragnet-spying-case-rejected-supreme-court, accessed December 7, 2022.

7 Franceschi-Bicchierai, L., "Lavabit's Forgotten Encryption Fight Looms Over the Apple Case.," March 18,, 2016, *Vice*, available at https://www.vice.com/en/article/gv5vg3/lavabit-snowden-forgotten-encryption-fight-looms-over-the-apple-fbi-case, accessed December 12, 2022.

By contrast, in February 2016, the FBI brought a court case against Apple, to force Apple to take steps to decrypt the work phone of the shooter in the San Bernardino massacre. Apple refused, and litigated the matter; the FBI then withdrew the request, having found a third-party provider of software that could decrypt the phone. The FBI found nothing of investigatory significance on the phone.[8] Crucially, however, the FBI, dealing with a globe-spanning tech firm with hundreds of millions of customers, did not ask Apple for its developer-level keys, which would have decrypted all Apple traffic.

In other words, larger firms, all else being equal, are better equipped to manage and resist public government surveillance demands, via court orders or other data requests, on the "front end" than small firms are. The risk to large firms of refusing such an order is not existential in the way that it can be for small firms like Lavabit. Smaller firms may find it harder than incumbents to respond to general privacy regulations, especially those that require the implementation of a consumer consent-based privacy framework.[9] In that sense, it seems clear that large telecommunications firms like AT&T and Verizon have the capacity to resist front-end government surveillance demands, even if it appears that in fact those firms have chosen instead to form a deep collaboration with the U.S. government.

There may be a strategic element to these kinds of interactions. A small firm like Lavabit may not have a large number of users in which the government takes a close investigatory interest. Small firms in general are likely to receive government data requests only infrequently, and are likely to not perceive a need to develop the expensive in-house skills needed to address them. Large firms will likely view their government interactions as a repeated game, with aspects reaching well beyond the question of whether to provide customer communications in cleartext. For example, by 2019, Amazon and Microsoft, two PRISM partners, had become the finalists in bidding on a ten-year, $10 billion Department of Defense cloud computing and AI program. A refusal by either firm to allow its servers to be transparent to PRISM might easily have disadvantaged Amazon or Microsoft in that bidding process.[10]

II. NATIONAL GOVERNMENT SURVEILLANCE MAY AFFECT THE NATURE OF INTERNATIONAL COMPETITION

One policy area where there is a known overlap between government surveillance practices and antitrust concerns is in the negotiations over U.S.-EU data sharing agreements, most often referred to as "Privacy Shield." We will briefly review the history of these agreements, and discuss the likely implications for competition policy.

The PRISM program, revealed in 2013 in the documents Edward Snowden brought out of the NSA, involves NSA exploitation of tech firm consumer communications on a mass scale, via the FBI's Data Intercept Technology Unit for explicit data requests, via co-optation of personnel internal to those companies, and via compromise of the encryption standards used by these firms.[11] As of 2013, PRISM was described as "the number one source of raw intelligence used for NSA analytic reports."[12]

One casualty of the PRISM revelation was what was then called the "Safe Harbor" agreement, which governed data flows between U.S.-headquartered and EU-headquartered companies. Under this agreement, U.S. companies could self-certify that they provided substantially equivalent privacy protections to their customers as EU companies provided to their customers. However, PRISM showed that U.S. tech companies were vulnerable to massive and systemic data exfiltration by the U.S. intelligence community.

An Austrian citizen, Max Schrems, brought suit in Ireland, arguing that this process of self-certification was now revealed to have been based on a lie, and that EU citizens could no longer rely on U.S. firms' self-certifications that those firms were protecting their rights. In 2015, the

8 See Tanfani, J., "Race to unlock San Bernardino shooter's iPhone was delayed by poor FBI communication, report finds," March 27, 2018, Los Angeles Times. Available at https://www.latimes.com/politics/la-na-pol-fbi-iphone-san-bernardino-20180327-story.html, accessed December 8, 2022.

9 See Campbell, J., A. Goldfarb, and C. Tucker (2015). Privacy regulation and market structure. Journal of Economics & Management Strategy 24(1), 47–73.

10 For the lengthy litigation history around this highly controversial contract, see Soper, T., "Pentagon cancels $10 billion JEDI cloud contract after long feud between Amazon and Microsoft," July 6, 2021, *Geekwire*, available at https://www.geekwire.com/2021/pentagon-cancels-10-billion-jedi-cloud-contract-long-feud-amazon-microsoft/, accessed December 12, 2022.

11 See Appelbaum, J. R. (2022). Communication in a world of pervasive surveillance: Sources and methods: Counterstrategies against pervasive surveillance architecture. [Phd Thesis 1 (Research TU/e / Graduation TU/e), Mathematics and Computer Science]. Eindhoven University of Technology, pp. 72-84.

12 See Madrigal, A., "Bombshell Report: NSA and FBI 'Tapping Directly' Into Tech Companies' Servers:
Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube, and Apple are all implicated." The Atlantic, June 6, 2013. Available at https://www.theatlantic.com/technology/archive/2013/06/bombshell-report-nsa-and-fbi-tapping-directly-into-tech-companies-servers/276633/, accessed December 7, 2022.

Court of Justice of the European Union agreed, and invalidated the Safe Harbor agreement.[13] U.S. and EU diplomats scrambled to replace it with the "Privacy Shield" agreement,[14] which the CJEU proceeded to invalidate in its turn.[15] The newest agreement, "Privacy Shield 2.0," was agreed in 2022; President Biden has issued an executive order implementing it,[16] but the text will not come into effect till 2023. That text is also likely to be litigated, and is unlikely to survive court review, because it does not appear to meet the CJEU's standards for providing meaningful redress to EU citizens whose privacy is invaded by these surveillance systems.[17]

The implications for competition policy are substantial. If U.S. tech firms appear as a result of U.S. government surveillance to no longer be trustworthy custodians of their citizens' data, one natural response of EU authorities will be efforts to promote data localization within the EU, up to and possibly including compelling U.S. tech firms to hive off separate firms to handle EU nationals' data under different firms.

In turn, speculatively, though the EU-based firms would then be under a legal obligation to follow CJEU requirements for data privacy, national governments within the EU might be more eager to pursue a "national champions" model to encourage locally owned competition to those U.S. firms, such as French-owned search engine competitors Qwant and Algolia, and to then form close collaborative relationships with these more domestically controllable firms. Of course, there is nothing that restricts these concerns to U.S. government surveillance in particular; the U.S. has just banned Chinese telecommunications products from Huawei, ZTE, Hytera Communications, Hikvision, and Dahua,[18] showcasing the same anxiety about dealing from afar with firms that are perceived as being trusted partners of their home country's intelligence services.

III. GOVERNMENT SURVEILLANCE POLICIES FAVOR INCUMBENTS DUE TO THE COSTS THEY IMPOSE

Most models of privacy and competition focus on how the costs that regulatory compliance imposes shapes competitive structures.[19] In general, the theoretical and empirical evidence in this research that shows consumer-focused privacy regulation leads to more contraction and deters entry. The mechanism that is usually documented is that firms have to manage data flows on a customer-level explicitly. This leads to fixed costs that are better borne by large firms. However, the same mechanism is also possible when it comes to regulation that is designed to enhance government surveillance of customer data.

"Know Your Customer" regulations were developed to inhibit money-laundering and other criminal activity. However, by emphasizing face-to-face contact and verification, they also operate to discourage privacy-enhancing financial innovations, and to safeguard the business model of existing, brick-and-mortar banks. In that sense, the substantial work being done on how to update KYC regulations should take into account the potential anti-competitive impacts of the current U.S. model.[20]

13 See *Maximilian Schrems v. Data Protection Commissioner* ("Schrems I"), ECLI:EU:C:2015:650, October 6, 2015, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=16990, accessed December 12, 2022.

14 See https://www.politico.eu/wp-content/uploads/2016/06/Privacy-shield-text-for-opinion-and-annexes.pdf, July 12, 2016, accessed December 12, 2022.

15 See *Maximilian Schrems v. Facebook Ireland Limited* ("Schrems II"), ECLI:EU:C:2020:559, July 16, 2020, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=16990, accessed December 12, 2022.

16 See "Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities," October 7, 2022, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/, accessed December 12, 2022.

17 See CMS Germany, "US adopts Executive Order to implement EU-US Data Privacy Framework," November 10, 2022, available at https://www.lexology.com/library/detail.aspx?g=211ffdc2-0d59-4ef8-9516-7310fa85ff9e, accessed December 7, 2022.

18 See Woolacott, E., "U.S. Bans Chinese Telecom Kit Over National Security Concerns," available at https://www.forbes.com/sites/emmawoollacott/2022/11/28/us-bans-chinese-telecom-kit-over-national-security-concerns/, accessed December 12, 2022.

19 Campbell J, Goldfarb A, Tucker C. Privacy regulation and market structure. Journal of Economics & Management Strategy. 2015 Mar;24(1):47-73. And Johnson G, Shriver S, Goldberg S. Privacy & market concentration: Intended & unintended consequences of the GDPR. Available at SSRN 3477686. 2022.

20 The literature here is extensive, but see, for example, Chorzempa, M., *"The Cashless Revolution: China's Reinvention of Money and the End of America's Domination of Finance and Technology,"* 2021.

IV. GOVERNMENT SURVEILLANCE PROGRAMS MAY AFFECT STANDARDS AND IN TURN COMPETITION

Conventional DOJ antitrust investigations have often focused on the standards-setting process in different industries, watching for situations where one company unfairly skews the standards-setting process to favor its own products and block its competitors'. With respect to government surveillance and encryption standards, the risk is fundamentally the same, with the difference that the standards-setting process may be skewed so as to permit unfair government access to citizens' data by a government intelligence agency. NSA's actions to "enable" national and international cryptographic standards are included under a program codenamed "BULLRUN."

This sabotage has included the explicit weakening of the DES cryptographic standard issued by NIST, with the collusion of IBM; the bribery of security industry pioneer RSA to include NSA-enabled cryptographic standards; NSA influence over the ISO/IEC standardization process; and presumably other as yet undisclosed actions through to the present.[21] Each of these interventions necessarily privileges some firms in the market over others, and in turn binds those firms in closer cooperation with the intelligence community, while depriving other, less favored firms of access to revenue from government sources.

V. IS ANY OF THIS AN ANTITRUST ISSUE?

Both the FTC and competition authorities in other countries have begun to consider privacy as a component of their competitive analysis for mergers. The EU, for example when examining the Microsoft/LinkedIn merger, described privacy in personal social networks as "an important parameter of competition."[22] The government's Horizontal Merger Guidelines explicitly allow competition authorities to consider "non-price terms and conditions that adversely affect customers, including reduced product quality, reduced product variety, reduced service, or diminished innovation."[23] However, it is problematic if the antitrust enforcement arm is part of a governmental entity that encourages firms to share data about citizens for surveillance purposes, and argues against strong encryption. We have seen little evidence that firms' sharing of data with governments, as opposed to data privacy practices in general, are becoming part of antitrust analysis, however.

There is reason for concern that current trends in government surveillance and information management may lead to anti-competitive outcomes, even if this concern fits poorly under the existing framework of U.S. antitrust law. We have presented historic examples that suggest that government surveillance programs may give governments incentives to work with large established incumbents. However, it is not within the scope of this article to analyze those incentives empirically, and we encourage further work in this area.

---

21 See Ashur, T., Luykx, A. (2021). "An Account of the ISO/IEC Standardization of the Simon and Speck Block Cipher Families" in Avoine, G., Hernandez-Castro, J. (eds) Security of Ubiquitous Computing Systems. Springer, Cham. https://doi.org/10.1007/978-3-030-10591-4_4; Menn, J., "Exclusive: NSA infiltrated RSA security more deeply than thought - study," March 31, 2014, Reuters, available at https://www.reuters.com/article/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331, accessed December 8, 2022; and Appelbaum, J. R. (2022). Communication in a world of pervasive surveillance: Sources and methods: Counterstrategies against pervasive surveillance architecture. [Phd Thesis 1 (Research TU/e / Graduation TU/e), Mathematics and Computer Science]. Eindhoven University of Technology, pp. 72-84.

22 See Cooper, James C., Antitrust & Privacy (November 11, 2020). The Global Antitrust Institute Report on the Digital Economy 32, available at SSRN: https://ssrn.com/abstract=3733752 or http://dx.doi.org/10.2139/ssrn.3733752.

23 See Department of Justice & Federal Trade Commission, Horizontal Merger Guidelines (2010).

CPI COMPETITION POLICY® INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.