

## MIT Open Access Articles

### *The impact of online surveillance on behavior*

The MIT Faculty has made this article openly available. **Please share** how this access benefits you. Your story matters.

**Citation:** Marthews, Alex & Catherine Tucker. "The impact of online surveillance on behavior." The Cambridge handbook of surveillance law, part 3 (June 2017): 393-508 © 2017 The Author(s)

**As Published:** 10.1017/9781316481127.019

**Publisher:** Cambridge University Press

**Persistent URL:** <https://hdl.handle.net/1721.1/130532>

**Version:** Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

**Terms of use:** Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.



## 18 The Impact of Online Surveillance on Behavior

Alex Marthews<sup>†</sup> & Catherine Tucker<sup>‡</sup>

Mass digital surveillance differs from older, analog, and more overt forms of physical surveillance. Nonetheless, empirical research after the Snowden revelations shows that it still has a meaningful chilling effect on online behavior, including Google searches, use of Wikipedia, and expression of controversial opinions. In the courts, these studies may help plaintiffs challenging mass surveillance programs in both the United States and the European Union to demonstrate standing. In the executive and legislative branches, the studies enable the discussion to move on from the question of whether a chilling effect exists from surveillance, to the question of what, if anything, to do about it.

### I How Online Surveillance May Affect Behavior Differently from Offline Surveillance

A common trope in surveillance debates claims that subjects of digital surveillance are less affected than subjects of more traditional direct surveillance. A driver might panic and hit the gas at the sight of a police cruiser parked along the side of the road, but the same driver might not much care about or respond to the kinds of mass surveillance programs revealed by the Snowden documents. This skepticism stems mainly from an accurate perception that overt, individualized analog surveillance conveys a stronger signal of interest by the government in a particular citizen's activities than does mass digital surveillance, which by definition is general rather than particular.<sup>1</sup>

Conventional surveillance prior to the broad adoption of the Internet tended to involve intense physical surveillance of individuals by other individuals. This is costly and labor-intensive; even states such as the former East Germany, which employed both overt and covert physical surveillance on a grand scale, were only able to keep dossiers on a little more than one-third of their people.<sup>2</sup> Physical surveillance, the cultivation of informants,



<sup>†</sup> Alex Marthews is the National Chair of Restore the Fourth, [CE: rt4chair@protonmail.com].

<sup>‡</sup> Catherine Tucker is the Sloan Distinguished Professor of Management Science and Professor of Marketing at MIT Sloan, cetucker@mit.edu, and Research Associate at NBER.

<sup>1</sup> For the purposes of this discussion, we consider collection of data to be “mass surveillance” if it is not particularized to a particular investigatory target and his or her direct associates in a criminal enterprise, rather than adopting the perspective of the U.S. government and others that collection of data is not “mass” so long as it involves the use of some selector prior to collection.

<sup>2</sup> Joel D. Cameron, *Stasi*, ENCYCLOPEDIA BRITANNICA (Apr. 14, 2015), <http://www.britannica.com/topic/Stasi>.

and infiltration of dissident groups by undercover police officers continue,<sup>3</sup> have in some respects expanded,<sup>4</sup> and are still highly controversial. But the digital superstructure of surveillance has become, since the advent of the Internet, both much more pervasive than offline surveillance and much more understandable using empirical methods than it was before.

In the area of communications surveillance, analog methods tended to require a physical tap on individual phones or the physical reading of individual envelopes and letters, so, in practice, it was also knowably harder and more expensive on a per-individual basis than mass digital surveillance is today. Surveillance agencies and the political leaders who defend them are often at pains to stress this difference,<sup>5</sup> arguing that mere collection of communications metadata on all citizens does not really constitute surveillance until an individual human agent looks at the results of a query on a particular person or pattern of behavior, as happens in a small percentage of the overall data points collected.<sup>6</sup>

Digital surveillance's impact on a given individual may on average be smaller than the impact of analog surveillance on a given person physically followed, because it is more diffuse and inherently covert in nature. However, it also offers important advantages to researchers interested in the effects of surveillance on individuals. To an extent, if mass digital surveillance is so relatively unobtrusive that it is possible to be surveilled and be only marginally aware of it day to day, then empirically measuring the effect of such systems on behavior could provide a lower bound for the effects of surveillance in general. Furthermore, the high trackability of online behavior allows us to determine the impact of surveillance most clearly in the context of online behavior, using information on search terms used and Web sites visited to demonstrate empirically the existence of a chilling effect on citizens' free expression and association online.

## II Chilling Effects and Legal Approaches to Measuring Impacts of Surveillance

It is this technological change – this digitization of the streams of our thoughts and actions – that leads to surveillance's being not only more prevalent in the abstract but more realistically litigatable in the particular. Professor Frederick Schauer argued in 1978 that the chilling effects of his day were “likely unprovable” and so argued for a conceptual rule whereby the courts would err in favor of the freedom of speech of “over-cautious” speakers that would not require individualized proof of actions not taken or thoughts not expressed.<sup>7</sup> Professor Vincent Blasi went further in 1987, condemning

<sup>3</sup> Gilbert Ramsay et al., *Report: Impacts of Surveillance on Contemporary British Activism*, OPENDEMOCRACYUK (May 24, 2016), <https://www.opendemocracy.net/uk/gilbert-ramsay/report-impacts-of-surveillance-on-contemporary-british-activism>.

<sup>4</sup> *Terror Probes Have FBI's Informant Numbers Soaring*, NPR (Aug. 21, 2011, 5:10 PM), <http://www.npr.org/2011/08/21/139836377/the-surge-in-fbi-informants>.

<sup>5</sup> Herbert Lin, *Having a Conversation about Bulk Surveillance*, 59 COMM. OF THE ACM 2, 40 (2016).

<sup>6</sup> Perhaps the best available estimate is from internal documents showing data processing of MI5's “Preston” program, which indicate that perhaps 3 percent of the information gathered is viewed by a human agent, and a much smaller percentage than that is synthesized into meaningful “end product.” Ryan Gallagher, *Facing Data Deluge, Secret U.K. Spying Report Warned of Intelligence Failure*, INTERCEPT (June 7, 2016, 4:38 AM), <https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/>.

<sup>7</sup> Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the Chilling Effect*, 685 B.U. L. REV. 730–31 (1978).

even the idea of chilling effects of surveillance as being based on “crude behavioral speculation.”<sup>8</sup>

American courts in the predigital era generally, though not without controversy, adhered to this view that chilling effects were speculative. In *Laird v. Tatum*, the 1972 U.S. Supreme Court dismissed, by a 5–4 vote, the claims of the director of an advocacy group for conscientious objectors that he was subject to army surveillance in his political activities, opining that “allegations of a subjective ‘chill’ are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm.”<sup>9</sup> Citing *Laird*, in 2013 in *Clapper v. Amnesty International*, another divided 5–4 Court likewise condemned the idea that the respondents could “manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.”<sup>10</sup> Both Courts thus dismissed the cases on standing grounds.

The privacy expert Daniel Solove (2007) accurately characterizes the conundrum faced by courts in such cases:

Determining the existence of a chilling effect is complicated by the difficulty of defining and identifying deterrence. It is hard to measure the deterrence caused by a chilling effect because it is impossible to determine with certainty what people would have said or done in the absence of the government activity. Often, the primary evidence will be a person’s own assertions that she was chilled, but merely accepting such assertions at face value would allow anyone claiming a chilling effect to establish one. At the same time, demanding empirical evidence of deterrence is impractical because it will often be impossible to produce.<sup>11</sup>

### III The Snowden Revelations

On June 6, 2013, new information emerged about U.S. government surveillance practices based on top-secret documents leaked by the NSA contractor and systems administrator Edward Snowden. These contained revelations about the PRISM program (now termed “downstream”), which was [redacted] In a statement indicating their termination of “about” collection on April 28, 2017, NSA noted this program name change. However, we have retained the term “PRISM” in the remainder of the chapter text, because our analysis was conducted while the program had that name.] a code name for a mass electronic surveillance data mining program managed by the National Security Agency (NSA). The NSA’s slides disclosed partnerships of a kind with nine major tech companies, including

<sup>8</sup> Vincent Blasi, *Pathological Perspective and the First Amendment*, 85 COLUM. L. REV. 449, 482 (1985).

<sup>9</sup> 408 U.S. 1, 13–14 (1972).

<sup>10</sup> 133 S.Ct. 1138, 1151 (2013). The *Clapper* Court relied on assertions by Solicitor-General David Verrilli that if data derived from mass surveillance were used against a defendant in court, that defendant would be notified of that fact and would be able to challenge the basis of that surveillance. Reply Brief for the Petitioners at 15, *Clapper v. Amnesty Int’l*, 133 S.Ct. 1138 (2013) (No. 11–1025), [http://www.americanbar.org/content/dam/aba/publications/supreme\\_court\\_preview/briefs/11-1025\\_pet\\_reply.authcheckdam.pdf](http://www.americanbar.org/content/dam/aba/publications/supreme_court_preview/briefs/11-1025_pet_reply.authcheckdam.pdf). The Court then used the absence of such notices as evidence that mass surveillance was not sufficiently prevalent for the claim of standing to be credible, not realizing – as Verrilli found out shortly afterward – that it was not in fact true that the government did notify defendants of the use of surveillance-derived data. Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. TIMES (July 15, 2013), [http://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html?\\_r=0](http://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html?_r=0).



<sup>11</sup> Daniel J. Solove, *First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV 112, 155 (2007).

Microsoft, Google, Yahoo!, AOL, and Skype, through which the NSA was able to obtain real-time data content.<sup>12</sup> In the intervening months and years, many further disclosures from the same set of leaked documents have refined and expanded our understanding of how these programs work. In our study “Government Surveillance and Internet Search Behavior,”<sup>13</sup> we studied the impact of the revelations as a whole on people using Google search, therefore beginning at the point of initial disclosure on June 6. Later disclosures suggest that the NSA slides may have overstated the official nature of its partnerships with the companies named; arguments continue over the extent to which PRISM collection is voluntary or involuntary. However, NSA internal documents attest that PRISM constituted a very large proportion – 91 percent, as of mid-2011<sup>14</sup> – of the signals intelligence data gathered by the NSA. Later disclosures relating to other programs such as TEMPORA or tools such as XKEYSCORE could also, for highly informed users, have further affected their search behavior. However, our study considers the impact on search behavior among the general public after the publicization of the general fact of government mass surveillance, rather than the unpublicized operation of the programs themselves, so the distinctions among these programs, while substantial, will not be material for our analysis.

The Snowden revelations provoked controversy, both from domestic privacy activists and from international governments who were concerned about the privacy of their own citizens given the worldwide reach of the data collection. The U.S. government emphasized in its initial response that the “authority [under which the program falls] was created by the Congress and has been widely known and publicly discussed.”<sup>15</sup> But it was not generally understood prior to June 2013 that the authority in question, Section 702 of the FISA Amendments Act, authorized consumer data held by such companies, including data on individuals’ search behavior, to be made available to the U.S. government on a mass rather than an individualized basis. Various efforts are under way in Congress to reform this authority, in advance of its next sunset date in December 2017.

It was immediately apparent when the Snowden revelations began that they were different in kind from previous surveillance-related revelations, such as those of William Binney<sup>16</sup> or Russell Tice.<sup>17</sup> Unlike these previous whistle-blowers, Edward Snowden took away with him internal documents of unquestionable authenticity that attested to the existence of surveillance programs that were near-universal in scope. Consequently, his evidence was more likely to push courts to recognize the plausibility of surveillance

<sup>12</sup> Earlier that morning, the “Verizon scandal” had disclosed to the public that phone companies, including Verizon Wireless, had been ordered by a secret court continually to disclose the metadata associated with all calls – location, caller, caller identification, and call duration.

<sup>13</sup> Alex Marthews & Catherine Tucker, *GOVERNMENT SURVEILLANCE AND INTERNET SEARCH BEHAVIOR* (2017).  We have uploaded a substantially updated and expanded version of this paper, at the same URL.  has necessitated some substantive changes to this chapter.], [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2412564](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564).

<sup>14</sup> John W. Rollins & Edward C. Liu, *NSA SURVEILLANCE LEAKS: BACKGROUND AND ISSUES FOR CONGRESS* 4 (2013).

<sup>15</sup> Director of National Intelligence, *FACTS ON THE COLLECTION OF INTELLIGENCE PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 1* (2013), <https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf>.

<sup>16</sup> See Newton Lee, *COUNTERTERRORISM AND CYBERSECURITY* 153 (2013).

<sup>17</sup> See *EXCLUSIVE: National Security Agency Whistleblower Warns Domestic Spying Program Is Sign the U.S. Is Decaying into a “Police State,”* Democracy Now! (Jan. 3, 2006), [http://www.democracynow.org/2006/1/3/exclusive\\_national\\_security\\_agency\\_whistleblower\\_warns](http://www.democracynow.org/2006/1/3/exclusive_national_security_agency_whistleblower_warns).

litigants' standing claims – namely, that mass surveillance could produce individual claims that were cognizable as “injury in fact.” Four [redacted]: Given the publication date of the Handbook, it would be appropriate to update the [redacted] number] years after the initial Snowden revelations, the legal effects were mixed, but they are still far-reaching. In the European Union, Max Schrems was able to bring a case before the European Court of Justice that invalidated the Safe Harbor agreement under which U.S. and EU firms share data.<sup>18</sup> Schrems expressly relied on the Snowden revelation of the PRISM program to allege injury to his privacy rights under Article 8 of the European Convention on Human Rights. In the U.S. Second Circuit Court of Appeals, the Snowden revelations led to a decision that a mass metadata surveillance program conducted under USA PATRIOT Act Section 215 was not in fact authorized by that statute as it then read.<sup>19</sup> A modified form of the program was shortly afterward authorized by the USA FREEDOM Act of 2015.<sup>20</sup> In *Klayman v. Obama*, plaintiffs were awarded standing to challenge surveillance of their communications in part on the basis of information contained in the Snowden documents, but the passage of the USA FREEDOM Act mooted their challenge for prospective relief from the surveillance under the 215 program – a risk that reformers and legal scholars were well aware of prior to its passage –<sup>21</sup> in that the surveillance conducted after that act passed now differed materially from the program described in the Snowden files. In *Wikimedia Foundation v. NSA*, the plaintiffs alleged that the NSA's “upstream” collection of all Americans' international communications, including emails, Web-browsing content, and search engine queries, violated the First and Fourth Amendments of the U.S. Constitution. [redacted] the U.S. District Court for the District of Maryland dismissed the suit for lack of standing.<sup>22</sup> What these cases show is that courts may still, even after Snowden, be institutionally reluctant to award standing to individual plaintiffs when the ramifications of actually shutting down aspects of government mass surveillance programs become apparent.<sup>23</sup>

Paradoxically, we can see that the very breadth and scale of government mass surveillance programs act to insulate them. It is relatively easier to overrule the government on the surveillance of a particular individual, as would have been authorized by the Foreign

<sup>18</sup> Case C-362/14, *Schrems v Data Protection Comm'r*, (Oct. 6, 2015), <http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN>.


<sup>19</sup> *Am. Civil Liberties Union v. Clapper*, 785 F.3d 787, 829 (2d Cir. 2015).

<sup>20</sup> Pub. L. No. 114–23, 129 Stat. 268.

<sup>21</sup> See Steven Nelson, *Freedom Act's Advance Threatens NSA Court Cases: Obama's Signature Could Spare the Government a Courtroom Reckoning, Legal Experts Say*, US NEWS & WORLD REPORT (Nov. 14, 2014), <http://www.usnews.com/news/articles/2014/11/14/freedom-acts-advance-threatens-nsa-court-cases>. The USA FREEDOM Act contained some elements of reform, some of modernization, and some of expansion, rendering analysis of its effects especially vexed. However, it is critical to observe that the Section 215 mass metadata program represented a very small proportion of overall U.S. government surveillance. More than 90 percent of data gathered are estimated to be gathered under the PRISM program, which is the one whose effects on user search behavior we analyze and which is authorized under a different U.S. law, Section 702 of the FISA Amendments Act of 2008. Pub. L. No. 110–261, 122 Stat. 2436, § 702.

<sup>22</sup> *Wikimedia Found. v. Nat'l Sec. Agency*, 143 F. Supp. 3d 344 (D. Md. 2015), documents at <https://www.aclu.org/legal-document/wikimedia-v-nsa-d-md-opinion>.

<sup>23</sup> *Id.* at 351 (quoting *Clapper v. Amnesty Int'l*, 133 S.Ct. 1139, 1157 (2013) (“Importantly, the standing inquiry is ‘especially rigorous when reaching the merits of the dispute would force [a court] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional,’ particularly ‘in the fields of intelligence gathering and foreign affairs’”).

Intelligence Surveillance Court in the 1970s and 1980s, because one individual can only inflict a relatively small amount of harm. However, shutting down a whole surveillance program, even on the grounds of a constitutional violation, begins to look like judicial activism, and courts would on the whole still prefer to see legislators act to rein in the abuses than to leave it up to them.<sup>24</sup> This may then be compounded further by a chilling effect among legislators. The apparatus of congressional oversight of surveillance programs limits specific knowledge of secret surveillance programs to the members, and sometimes only to the chair and ranking member, of the Senate and House Intelligence Committees, forcing ordinary lawmakers to defer to the expertise of lawmakers who may themselves be chosen by leadership for their sympathy to intelligence community concerns. More worryingly, if the allegations of Russell Tice were true, and are still operative, that the NSA specifically targets for surveillance lawmakers, political candidates, and judges who might have authority to regulate its activities or budget,<sup>25</sup> legislators may feel directly chilled from acting to regulate intelligence agencies by the potential for their own careers to be damaged by the disclosure of embarrassing secrets.<sup>26</sup> The questions of what political surveillance is conducted in the United States, and especially the extent to which NSA data may properly be exploited by White House staff, have resurfaced vividly with the allegation made in March 2017 by President Trump that his campaign was “wiretapped” by his predecessor, and the upcoming sunset in December 2017 of the FISA Amendment Act authorities under which both ‘downstream’ (=PRISM) and ‘upstream’ collection is conducted. : We view this addition in the text as usefully replacing the now somewhat outdated footnote 26.]

Given this legal and political landscape in the United States, it would be exceptionally useful to both courts and policy makers if researchers were able to document empirically some of the actual effects of surveillance on individuals’ behavior. It was immediately clear to us as researchers that the Snowden revelations represented the kind of exogenous

<sup>24</sup> See *United States v. Jones*, 132 S.Ct. 945, 964 (2012) (Alito, J., concurring) (“In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way”) (internal citation omitted).

<sup>25</sup> “Okay. They [the NSA] ... went after members of Congress, both Senate and the House, especially on the intelligence committees and on the armed services committees and ... judicial. But they went after other ones, too. They went after ... heaps of lawyers and law firms. They went after judges. One of the judges [Samuel Alito] is now sitting on the Supreme Court that I had his wiretap information in my hand. Two are former FISA court judges. They went after State Department officials. They went after people in ... the White House – their own people. They went after antiwar groups. They went after U.S. ... companies that that do ... business around the world. They went after U.S. banking firms and financial firms that do international business. They went after NGOs ... like the Red Cross that that go overseas and do humanitarian work. They went after a few antiwar civil rights groups. So, you know, don’t tell me that there’s no abuse, because I’ve had this stuff in my hand and looked at it. And in some cases, I literally was involved in the technology that was going after this stuff. And you know, when I said to [former MSNBC show host Keith] Olbermann, I said, my particular thing is high tech and you know, what’s going on is the other thing, which is the dragnet. The dragnet is what Mark Klein is talking about, the terrestrial dragnet. Well my specialty is outer space. I deal with satellites, and everything that goes in and out of space. I did my spying via space. So that’s how I found out about this.” *NSA Whistleblower: NSA Spying on – and Blackmailing – Top Government Officials and Military Officers*, FOX NATION (June 20, 2013), <http://nation.foxnews.com/2013/06/20/nsa-whistleblower-nsa-spying-%E2%80%93-and-blackmailing-%E2%80%93-top-government-officials-and-military>.

<sup>26</sup>

shock that could be used to gain a much more precise understanding of the effects of knowledge or fear of surveillance on behavior than had been possible for decades.<sup>27</sup> The Snowden revelations began at a defined point, were very broadly reported across the world, and related only to the topic of surveillance. Thus, unlike for the Watergate scandal of the 1970s or the fall of the German Democratic Republic in 1989, reactions to the Snowden revelations could plausibly be attributed to shock specifically from surveillance, as opposed to shock from a spectrum of abusive governmental behavior including surveillance. Such a “clean” shock is unlikely to occur again in the near future. It therefore presented, and continues to present, a uniquely rich research opportunity.

Within the first six months after the Snowden revelations began to break, it appeared that the only information becoming available regarding any potential chilling effects was survey based. Opinion polling on the topic in June 2013 by the Pew Internet & American Life Project did not at that stage focus on changes in behavior.<sup>28</sup> A contemporaneous PEN America survey focused on the effects on writers in particular, with 28 percent of writers reporting “curtailed social media activities” in response to the Snowden revelations, 24 percent reporting that they “deliberately avoided certain topics in phone or email conversations,” and 16 percent reporting that they “avoided writing or speaking about a particular topic.”<sup>29</sup> Of course, the survey approach – while quick relative to well-constructed empirical work – suffers from significant limitations. Writers may have been subject to substantial social desirability bias,<sup>30</sup> feeling that they *ought* to say that they responded in some meaningful way to knowledge that their writings were under more government scrutiny than they had supposed, even if they in fact had not responded. There was no indication that methods to reduce social desirability bias were employed in this study. Castro reports the results of a Cloud Security Alliance survey conducted in June and July of 2013 of its members, who are industry practitioners, companies, and other cloud computing stakeholders, about their reactions to the NSA leaks.<sup>31</sup> For non-U.S. residents, 10 percent of respondents indicated that they had canceled a project with a United States–based cloud computing provider and 56 percent said that they would be less likely to use a United States–based cloud computing service.<sup>32</sup> For U.S. residents, slightly more than one-third (36 percent) indicated that the NSA leaks made it more difficult for them to do business outside the United States.<sup>33</sup> The 10 percent reporting actual

<sup>27</sup> This, of course, evokes the famous prison proposed by Jeremy Bentham in Panopticon, or, the Inspection-house:

The more constantly the persons to be inspected are under the eye of the persons who should inspect them, the more perfectly will the purpose of the establishment have been attained. Ideal perfection, if that were the object, would require that each person should actually be in that predicament, during every instant of time. This being impossible, the next thing to be wished for is, that, at every instant, seeing reason to believe as much, and not being able to satisfy himself to the contrary, he should *conceive* himself to be so.

Jeremy Bentham, PANOPTICON; OR, THE INSPECTION HOUSE, 3 (1791) (emphasis in original).

<sup>28</sup> Pew Research Center, Few See Adequate Limits on NSA Surveillance Program (2013), <http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/>.

<sup>29</sup> Pen American Center, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR 3 (2013), [https://pen.org/sites/default/files/Chilling%20Effects\\_PEN%20American.pdf](https://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf).

<sup>30</sup> Robert J. Fisher, *Social Desirability Bias and the Validity of Indirect Questioning*, 20 J. CONSUMER RESEARCH 303 (1993).

<sup>31</sup> DANIEL CASTRO, HOW MUCH WILL PRISM COST THE U.S. CLOUD COMPUTING INDUSTRY? (2013), <http://www2.itif.org/2013-cloud-computing-costs.pdf>.

<sup>32</sup> *Id.* at 3.

<sup>33</sup> *Id.*



contract cancellation provides stronger evidence of an economic chill than the 56 percent thinking that they might have to not use, or cancel a project with, a U.S. provider in the future; but no follow-up was conducted with either group to establish what contracts were canceled or whether decisions not to use U.S. providers were in fact made.

We do not suggest that it is entirely meaningless that writers and cloud security professionals reported that they had made changes at this level or were thinking of doing so. Stating publicly that you intend to behave in line with a societal expectation both attests to the existence of that societal expectation and may itself act to shape behavior via formation of a stronger social norm. Not finding evidence of a behavioral change in the short term therefore would not necessarily exclude the possibility that this longer-term process would work slowly outward from intent to action.

#### IV How Did the Snowden Revelations Affect Search?

We believe that the strongest and best evidence of the effect of a sharp increase in knowledge of surveillance is empirical measurement of actual behavioral changes that can reasonably be said to have been caused by a particular shock.<sup>34</sup> Fortunately for our purposes, Google makes publicly available Google Trends, a data source covering all search terms entered by individual users across the world. Google Trends has been used in other studies to predict economic and health behaviors.<sup>35</sup> It does not provide raw search volumes or individually identifiable data, but instead is an index of a particular search term's popularity in a given region relative to other regions.

What follows is a summary of the paper that we wrote on this topic using Google Trends data.<sup>36</sup> Readers who are interested in more technical details about the exact empirical methodology can consult the full paper.

We confronted the question of how people perceived the likelihood of their searches' triggering interest from the U.S. government in the following fashion. We required some external source of search terms of potential interest to the U.S. government. Fortunately, such a list does exist in the public domain; it is provided for the use of analysts working in

<sup>34</sup> As a further note on longer-term norm formation and economic effects, now that four years have passed, we can see the longer-term formation of a stronger social norm in the technology industry in favor of end-to-end encrypted products and more aggressive discarding of data, which is surely strongly influenced by the Snowden revelations, though not in ways that are easily measured using empirical techniques. Indeed, if technology companies were to adopt stronger data practices, and their sales were to rise as a result, we might be in the strange position of effectively arguing that mass surveillance, by giving rise to the Snowden revelations and thereby to stronger data practices and higher sales for such companies, had provided economic benefits. Equally, if sales by United States- or UK-based firms were to suffer, because they were perceived as being insecure, and sales of firms based in other countries were to rise, because they were perceived as being more secure, we cannot argue that this means that mass surveillance is economically damaging in a general sense, but only insofar as it inflicts reputational costs disproportionately on companies wittingly or unwittingly participating in mass surveillance systems, and thereby potentially disproportionately on particular countries rather than others. That assessment, however, would obscure the high level of variation in data security practices within countries, and even within firms in the case of firms with multiple products.

<sup>35</sup> Hyunyoung Choi & Hal Varian, *Predict the Present with Google Trends*, 88 *ECON. REC.* 2 (2012); Herman Anthony Cameiro & Eleftherios Mylonakis, *Google Trends: A Web-Based Tool for Real-Time Surveillance of Disease Outbreaks*, 49 *CLINICAL INFECTIOUS DISEASES* 1157 (2009).

<sup>36</sup> Alex Marthews & Catherine Tucker, *GOVERNMENT SURVEILLANCE AND INTERNET SEARCH BEHAVIOR* (2015), [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2412564](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564).

the Media Monitoring Capability section of the National Operations Center, an agency under the Department of Homeland Security (Table A.1).<sup>37</sup> The list was made public in 2012 and continued to be used and reproduced within the Department of Homeland Security (DHS) up to the time of the Snowden revelations.<sup>38</sup> As far as we are aware, it remains in effect today, though we cannot be certain that no changes have been made. It is therefore the most relevant publicly available document for assessing the kinds of search terms that the U.S. government might be interested in collecting under PRISM or under its other programs aimed at gathering Google search data, even though it is focused on surveillance of social media Web sites rather than search engines. As far as we are aware, neither the DHS nor any other surveillance agency has revealed or has had leaked its list of search terms that would raise flags for searches on Google itself.<sup>39</sup> Later, we use independent raters on Mechanical Turk to evaluate whether users perceive particular search terms as likely to get you in trouble with the U.S. government.

Second, we used a crowdsourced list of embarrassing search terms (Table A.2). Our overall aim in establishing a reasonable list of “embarrassing” terms was to find terms that would not implicate national security issues of interest to DHS, or duplicate any term found in that list, but which would instead cause embarrassment for most people if third parties found out about those searches.<sup>40</sup> We were also seeking a list that had a broad range of terms, rather than simply being sexual in nature. We crowdsourced a group of participants who were part of the local technology community. The participants were young (twenties and thirties), well educated, and balanced equally between men and women. The list is the result of that process. Examples of terms included in this list are “white power,” “erectile dysfunction,” and “My Little Pony.”

We also needed a list of neutral search terms to use as a control. We also wanted to obtain a list of more “neutral” search terms to use as a quasi-control (Table A3), that were plausibly treated less intensively by the revelations about PRISM. To find a more neutral set of search terms, we turned to the nature of Google as a search engine. Users across the world use Google to search for local services and businesses. This type of search behavior provides a reasonable baseline measure of usage of search engines. To obtain words to capture this behavior, we first obtained a list of the most common local businesses in the US based on the North American Industry Classification System. We associated this list

<sup>37</sup> Department of Homeland Security, ANALYST’S DESKTOP BINDER 20–23 (2011), <https://epic.org/foia/epic-v-dhs-media-monitoring/Analyst-Desktop-Binder-REDACTED.pdf>.


<sup>38</sup> DEPARTMENT OF HOMELAND SECURITY, ANALYST’S DESKTOP BINDER, 18–21 (2013), <https://assets.documentcloud.org/documents/1086613/dhs-noc-mmc-analyst-desktop-foia-1340-redacted.pdf>.

<sup>39</sup> The list itself is in some ways not what people might expect. It includes, for example, the terms “agriculture” and “cloud,” perhaps out of concerns over terrorism directed at the food supply. But it is hard to see how the mention of “agriculture” in a social medium posting is in itself suspicious. The list also reads as if it was constructed with an analyst’s idea of what was relevant, rather than constructing a plausible idea of what potential attackers might write in a social media post. For example, someone involved with organized crime is, we suspect, very unlikely to use the term “organized crime” in a posting on social media.

<sup>40</sup> We may not be able to assume safely that, either in the view of the intelligence agencies or in the minds of citizens, there is a bright-line distinction between politically and personally sensitive terms. Intelligence agencies have shown themselves willing to use personally embarrassing but not prosecutable information about surveillance targets to shape their behavior. Leaked documents that form part of the current scandal, for example, show the NSA recommending using the online pornography viewing habits of “radicalizers” to discredit them. Also, the strong similarity of ratings of political and personal sensitivity in our study suggests that citizens may not accurately distinguish the two in their minds, instead thinking of government surveillance as being similar in many ways to a parent looking over their shoulder.

with search terms that would plausibly capture these businesses, namely: Gym, restaurant, nursing home, thrift store, butcher, gardener, beauty salon, cleaners, childcare, arcade, movies and weather.

Using these three lists, we were able to analyze how close the relationship is between what Google users *perceive* to be searches that cause them to be recognized by the U.S. government and search terms that might actually result in their being flagged in some way by the algorithms developed by U.S. surveillance agencies. It is not clear, for example, why using the search term “agriculture” might be perceived by an average Google search user as more likely to call him or her to the attention of the U.S. government than the term “gardener,” but the first term is on the DHS list and the second is from the list of neutral businesses. Legally, in order to demonstrate standing to bring a claim against the U.S. government for its conduct of mass surveillance, it might be necessary to show that a specific search was likely to trigger actual U.S. government interest, whereas in order for a chilling effect to exist it is only necessary for a searcher to believe that it would.

In the survey, we asked participants to rate each term by how likely it is that it would “embarrass” them or “get them into trouble” with their family, their close friends, or the U.S. government. We also asked them to rate how privacy sensitive they considered the term, how much they would like to keep the search secret, and how likely they would be to try to delete their search history after using this term. We asked all these ratings on a 5-point Likert scale, where 1 reflects the least sensitive and 5 reflects the most sensitive rating. As might be expected, the terms on the DHS list are most likely to be rated as “getting you in trouble with the government,” at a mean value of 1.62 out of 5. The search terms from the “embarrassing” list were rated the most likely to embarrass the user with his or her family or close friends, at mean values of between 2.2 and 2.3 out of 5 in terms of whether they would embarrass the user if his or her close friends or family knew about them and whether the user would want to keep the search secret or delete their search history, but at a lower sensitivity value of 1.59 in terms of whether the search would get them into trouble with the government. The neutral terms were in general rated the least embarrassing, with mean sensitivity values ranging between 1 and 1.22 out of 5 on all measures. As our list of search terms is  sense random, we then performed further validation to ensure that the search terms did represent politically and personally sensitive topics.<sup>41</sup>

Overall, across the 41 countries we studied, we found that the Google Trends search index fell for “high government trouble” search terms by roughly 4 percent after the Snowden revelations. It was surprising to us to find any difference in the search terms traffic, because there had been significant doubts expressed as to whether any macro-level effect on search behavior would be observable as a result of shocks such as the Snowden revelations. In countries other than the United States, there was a smaller, but still significant, decline for search terms that raters thought would give them an above-average

<sup>41</sup> Even for search terms that people might think plausibly signify some sort of malevolent intent, such as “anthrax” and “pipe bomb,” the vast majority of the site traffic resulting from that search was to innocent destinations such as the Centers for Disease Control and Wikipedia. This may throw into question the utility of governmental efforts to flag Internet traffic unconnected to any predicate or suspicion that an individual is involved in criminal behavior; the evident risk is that government agencies will be snowed under with false positive findings deriving from innocent searches and mentions on social media, and will therefore inevitably miss “needles” that they might be more able to find by gathering less “hay.”

likelihood of getting in trouble with a friend. We used a battery of robustness checks to validate the results, including controlling for news coverage and using different time windows as a falsification check.

This was, for us, an unexpected result. We began this study with considerable skepticism about whether the surveillance revelations were capable of affecting search traffic at such a macrolevel in the countries concerned. It seemed very possible that we would see no empirically demonstrable effect, and would then be drawing on the political science literature on low-information voters and political apathy as a guide for why search behavior was not affected.<sup>42</sup>

A natural concern is whether other factors could plausibly have shifted user behavior in early June relating to these specific keywords. However, the keywords cover a large variety of topics, so another news story relating to a small portion of them, such as an extreme weather event (for the DHS search terms) or the holiday season (for the list of neutral business terms) is unlikely to have shifted behavior for the whole list. Similarly, if we are looking at user behavior across the world, it is less likely that a smaller story could affect user behavior in the same way as the Snowden leaks. The only plausible shifters would be Google-specific, i.e., whether there was an internal change in the way the search engine operated at the time that would have a coherent and similar effect on search behavior in multiple countries. We are not aware of any such change.

We used Google in our study because Google represents such a large share of the worldwide search market, at around 70 percent during this period. An effect on search activities that was not perceptible on Google would therefore leave most Internet users unaffected. Our work addresses the question of whether more privacy-conscious users simply shifted their searches away from Google and to more secure search engines, such as SafeSearch or DuckDuckGo. Take-up of these services indeed boomed after the surveillance revelations, but from such a small base that adoption of secure search engines can only represent a small proportion – at most, around 10 percent – of the effect that we identified. At any rate, this noticeable shift away from Google to search engines perceived as more secure from government surveillance in the wake of the Snowden revelations necessarily bolsters, rather than undermines, the broader finding that there is a measurable chilling effect of surveillance.

## V How Did the Snowden Revelations Affect Nonsearch Online Behavior?

Building on this work, and using the same DHS list and a very similar methodology, Jon Penney found a comparable chilling effect on traffic to Wikipedia pages dealing with topics relating to terrorism, which provides evidence that the effect we observed may extend beyond the large, though limited, universe of Google search results.<sup>43</sup> Other

<sup>42</sup> See Ilya Somin, *Deliberative Democracy and Political Ignorance*, 22 GEO. MASON U. CRITICAL REV. 253 (2010) [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1694650](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1694650).

<sup>43</sup> Jon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, Berkeley Tech. L. J. Vol. 31, No. 1, p. 117, 2016, [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2769645](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645). Soren Preibusch, *Privacy Behaviors after Snowden*, 58 COMM. OF THE ACM 48 (2015), authored by a researcher employed by Microsoft, attempts to disprove the effect we found, but tried to do so using search results from Bing, a Microsoft-created search engine with a low market penetration. The article did not address the potential for selection bias (that users of such a minor-league search engine might systematically differ from search engine users in general in their tastes for privacy or their online behavior). For example, Bing users may use Bing only because it is set as the default search engine, and may have a lower level of education or of

academics are investigating the same topic with respect to Twitter, but no papers have yet been published relating to that platform. Investigations examining the effect on social media posts on platforms such as Facebook and Instagram are problematic because these platforms allow users control over their privacy settings, which themselves are not necessarily exogenous to the surveillance revelations. Thus, data for those platforms are simultaneously harder to collect and more ambiguous when collected.

## VI Other Methods of Studying the Effect of Surveillance on Behavior

Although this particular empirical technique has proved to be an adaptable way to examine the effects of mass surveillance programs, that does not mean that there are no other interesting ways to get at this difficult problem. In the communications literature, for example, Elizabeth Stoycheff sets up a lab experiment that primes social media users through their terms of service agreements to expect that their social media usage will be surveilled.<sup>44</sup> She then finds that those who are so primed, and hold what they perceive to be opinions that are distant from mainstream opinion regarding U.S. airstrikes on ISIS in Iraq, are particularly likely to be deterred from posting their opinions. There is also a substantial surveillance studies literature using sociological methods to hypothesize the effects on society of mass government and commercial surveillance, but not to our knowledge focusing on the empirical quantification of such effects, so we do not consider it in this chapter.

## Conclusion

It has become possible, primarily as a result of the exogenous shock of the Snowden revelations and the increased scholarly attention devoted to this problem, to analyze more precisely the chilling effect of surveillance on people's behavior, and, with limitations, to quantify the extent to which people's actual behavior is altered in response to knowing more about the scale and nature of surveillance. This has important ramifications in the legal sphere for ongoing litigation relating to privacy violations, especially in the area of being able to demonstrate a legally cognizable injury that would enable courts to confer standing to bring suit. In the policy sphere, it enables the discussion to move on from the question of whether a chilling effect exists, to the question of what, if anything, to do about the chilling effect that exists.

technical literacy, which in turn may affect how much they adopted more sophisticated search techniques to avoid surveillance. Second, despite asserting that he was performing a "longitudinal" study, his work appears to be based on snapshots of overall Bing traffic at different points in time, which is not longitudinal. Third, he appears to have misinterpreted our study as being based on "survey data," leading him to overstate the originality of his own work.

<sup>44</sup> Elizabeth Stoycheff, *Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 J. Mass Comm. Q. 296 (2016).

## Appendix

Table A.1. Random One-Third Sample of DHS Search Terms

agent	1.1
agriculture	1.05
air marshal	1.74
alcohol tobacco and firearms	2
anthrax	2.76
antiviral	1.65
assassination	2.44
authorities	1.35
avian	1.24
bacteria	1.15
biological	1.25
border patrol	1.37
breach	1.63
burn	1.63
center for disease control	1.6
central intelligence agency	1.55
chemical	2.1
chemical agent	2.21
chemical burn	1.85
chemical spill	1.89
cloud	1.05
coast guard	1.3
contamination	1.7
cops	1.39
crash	1.22
customs and border protection	1.65
deaths	1.25
department of homeland security	1.55
dirty bomb	3.74
disaster assistance	1.37
disaster management	1
disaster medical assistance team	1.18
dndo	1.84
domestic security	2.15
drill	1.06
drug administration	1.79
drug enforcement agency	1.85
ebola	1.17
emergency landing	1.42
emergency management	1.76
emergency response	1.4
epidemic	1.68
evacuation	1.35

(continued)

explosion	2.2
explosion explosive	3.15
exposure	1.5
federal aviation administration	1.1
federal bureau of investigation	1.63
first responder	1
flu	1.58
food poisoning	1.6
foot and mouth	1.45
fusion center	1.75
gangs	1.56
gas	1.55
h1n1	1.44
h5n1	1.6
hazardous	1.61
hazmat	1.35
homeland defense	1.42
homeland security	1.75
hostage	2.06
human to animal	2.2
human to human	1.45
immigration customs enforcement	1.47
incident	1.47
infection	1.6
influenza	1.2
infrastructure security	1.75
law enforcement	1.3
leak	1.4
listeria	1.47
lockdown	1.7
looting	2.11
militia	1.89
mitigation	1.45
mutation	1.58
national guard	1.37
national laboratory	1.45
national preparedness	1.6
national security	1.79
nerve agent	3.21
north korea	1.75
nuclear	2.1
nuclear facility	2.42
nuclear threat	2.17
organized crime	2.32
outbreak	1.6
pandemic	1.42
pipe bomb	4

plague	1.68
plume	1.11
police	1.2
pork	1.16
powder white	2.3
prevention	1.15
public health	1.3
quarantine	2.15
radiation	1.85
radioactive	2.05
recall	1.39
recovery	1.3
red cross	1.2
resistant	1.5
response	1.1
ricin	2.6
riot	1.6
salmonella	1.26
sarin	2.89
screening	1.3
secret service	1.89
secure border initiative	1.55
security	1.21
shooting	1.9
shots fired	2.11
sick	1.1
small pox	1.79
spillover	1.11
standoff	1.47
state of emergency	1.4
strain	1.39
swat	1.55
swine	1.25
symptoms	1
tamiflu	1.5
task force	1.15
threat	1.7
toxic	1.44
transportation security administration	1.35
tuberculosis	1.2
united nations	1.2
u.s. citizenship and immigration services	1.5
vaccine	1.2
virus	1.4
wave	1.05
world health organization	1.22
<b>Mean</b>	<b>1.62</b>



Table A.2. *Embarrassing Search Terms*

abortion	2.3
acutane	1.26
acne	1.1
adultery	2.26
agenda 21	1.47
aids	1.63
alcoholics anonymous	2.11
alien abduction	1.4
animal rights	1.16
anonymous	1.18
atheism	1.45
bail bonds	1.55
bankruptcy	2
bittorrent	1.37
black panthers	1.6
body odor	1.63
breathalyzer	1.65
casinos	1.21
celebrity news	1.11
chemtrails	1.78
coming out	2.05
communism	1.37
conspiracy	1.37
cop block	1.35
cutting	2.75
debt consolidation	1.79
depression	2
divorce lawyer	1.65
drones	1.42
eating disorder	2
erectile dysfunction	2
escorts	2.6
feminism	1.11
filesharing	1.45
fireworks	1.2
food not bombs	1.45
gay rights	1.47
gender reassignment	2.11
ghosts	1.25
gulf of tonkin	1.32
guns	2.05
herpes	1.89
hitler	1.85
hoarding	1.45
honey boo boo	1.33

incontinence	1.45
islam	1.25
keystone	1.16
kkk	2.11
larp	1.74
liposuction	1.26
lolcats	1.16
lonely	1.68
lost cause	1.26
marijuana legalization	1.5
marx	1.42
my little pony	1.5
nickelback	1.85
nose job	1.6
occupy	1.7
online dating	2
pest control	1.17
peta	1.2
police brutality	1.25
polyamory	1.8
porn	1.95
pregnant	1.7
protest	1.61
psychics	1.65
revolution	1.4
sexual addiction	2.45
shrink	1.65
socialism	1.22
sovereign citizen	1.21
sperm donation	2.06
strip club	2.26
suicide	2.68
tampons	1.85
tax avoidance	1.9
therapist	1.45
thrush	1.17
torrent	1.28
transhumanism	1.47
turner diaries	1.74
tuskegee	1.16
unions	1.28
vaccines and autism	1.33
vegan	1.3
viagra	2.16
warts	1.55

(continued)

weed	2.11
weight loss	1.5
white power	3.05
white pride	2.47
wicca	1.8
witchcraft	1.84
world of warcraft	1.35
<b>Mean</b>	<b>1.64</b>

---

*Table A.3 Google Search Terms*

arcade	1
beautysalon	1.22
butcher	1.22
childcare	1
cleaners	1
gardener	1
gym	1
movies	1
nursing home	1
restaurant	1
thrift store	1
Weather	1
<b>Mean</b>	<b>1.04</b>

---