Kentucky Law Journal

Volume 103 | Issue 3 Article 6

2015

Surveillance at the Source

David Thaw
University of Pittsburgh

Surveillance at the Source

David Thaw[1]

Contemporary discussions concerning surveillance focus predominantly on government activity. These discussions are important for a variety of reasons, but they generally ignore a critical aspect of the surveillance-harm calculus—the source from which government entities derive the information they use. The source of surveillance data is the information "gathering" activity itself, which is where harms like "chilling" of speech and behavior begin.

Unlike the days where satellite imaging, communications intercepts, and other forms of information gathering were limited to advanced law enforcement, military, and intelligence activities, private corporations now play a dominant role in the collection of information about individuals' activities. Private entities operate social networks, instant messaging, e-mail, and other information systems, which now are the predominant means through which people communicate. Private entities likewise control the physical and wireless networks over which these systems communicate.

This short Article separates surveillance into information "gathering" activities and information "usage" activities and examines the distinct, standalone privacy-harming potential of each. It then argues that while modern government surveillance focuses primarily on usage activities, private corporations engage in information gathering activities and separately use that information in their profitable business activity. Additionally, the fact that they possess such information makes private corporations a logical "feed" for information used in government surveillance.

Profit-making efforts, unlike public functions, must advance the

[1] Assistant Professor of Law and Information Sciences, University of Pittsburgh; Affiliated Fellow, Information Society Project, Yale Law School.

The author thanks Lisa Austin, Adam Candueb, Jennifer Coffman, Leslie Francis, Woodrow Hartzog, Dennis Hirsch, Margot Kaminski, Raymond Ku, Jacqueline Lipton, William McGeveran, James Nehf, Neil Richards, Patricia Sanchez Abril, Sharon Sandeen, Lawrence Siry, Richard Warner, the other participants of the Kentucky Law Journal's Symposium on Data Privacy, and the other participants of the Midwest Privacy Law Scholars Roundtable for their valuable input on this piece. The author also thanks Benjamin Monarch and the other members of the *Kentucky Law Journal* for their valuable editorial input during the publication process of this Article.

This piece benefitted substantially from the research and editorial assistance of Krysti Williams.

All errors are the sole responsibility of the author.

interests of shareholder return, and can only consider privacy or similar concerns to the extent that those concerns are subject to regulation or can be justified as market-competitive. This Article argues that since neither exception is common, the primary incentives of private corporations are to gather and use as much information as possible, thereby increasing the probability of "chilling effects."

Failure to examine the role of private corporations in surveillance scholarship thus creates both an incomplete discussion of the harms of government surveillance and fails to include an essential element of harm. This Article briefly examines notable examples of contemporary surveillance and argues for the inclusion of private actors in surveillance-harm analysis.

INTRODUCTION

Discussions regarding the benefits and harms of government surveillance enjoy a long history. The recent surge in legal scholarship and policy debate highlight how these discussions combine the elements of surveillance activity and the parties involved into a single "harm calculus" to debate what should and should not be permissible. Doing so ultimately overlooks critical elements of that calculus, and results in an incomplete discussion that fails to evaluate all the risks and benefits of such activities.

Surveillance literature historically focused on government actors. Law enforcement and intelligence community agencies would conduct surveillance and act upon that information, within guidelines set by policymakers. Those guidelines focused the debate on striking a proper balance between public services and surveillance harms. This formulation made sense, perhaps, in the era when wiretaps were operated by government agencies, government satellites conducted remote imaging surveillance, and government personnel conducted line-of-sight observations.

In the era of Big Data, however, where an electronic record of nearly every action a user takes is retained by private sector entities, considering the various elements of "surveillance" as a single merged activity is incomplete. This outdated formulation conflates two critically-separable elements of surveillance: (1) *gathering* of information, which is the collection of information used for analysis; and (2) *usage* of information, which is the conduct of analysis on gathered information to draw conclusions and inform actions and responses.

Failing to disambiguate these two elements makes scholarly and policy discussions of the surveillance-harm calculus incomplete because it ignores the role of private actors who are not subject to the same policy balancing mechanisms. When the government performed both functions, we relied upon the existing Constitutional framework to ensure that a balancing test occurred. With the private sector having overtaken the vast majority of gathering activities, however, the balancing equation is no longer complete. At best, the discussion fails to include the balancing mechanism for private actors—a healthy, functioning market

with adequate consumer choices. At worst, if the market fails, no balancing occurs at all, and discussions of the surveillance-harm calculus likely provide a false sense of resolution.

This Article puts forth two issues for consideration. First, that legal and policy literature has failed to adequately consider surveillance in the context of its two component activities—gathering and usage. Second, that this literature has failed to address the role of private actors in the government surveillance-harm calculus. It proceeds in two Parts. Part I addresses the lack of distinction between gathering and usage and proposes a modest framework for consideration. Part II addresses the role of private actors in surveillance. It juxtaposes traditional surveillance with modern surveillance, identifies the roles of private actors, and compares the balancing mechanisms for government and for private actors. It then identifies the risks associated with an incomplete discussion of the surveillance-harm calculus. This Article concludes by proposing a planned qualitative empirical project to compare a more comprehensive set of surveillance activities, their respective balancing mechanisms, and what gaps exist in current law to maintain the type of balancing tests for surveillance our social framework anticipates.

I. GATHERING VS. USAGE

This Part begins with the assertion that surveillance should be separated into two distinct types of activities for purposes of harm analysis. The first category encompasses activities involving the *gathering* of information—the actual "collecting" of data about individuals, organizations, governments, and their activities. The second category encompasses activities involving the *usage* of information—this can range from simple retention for administrative purposes to targeted, comprehensive analysis designed to track and predict the most personal and private aspects of an individual's life.

A brief review of the existing legal scholarship on privacy finds a curious lack of discussion regarding this distinction. Some scholars have posited more fine-grained distinctions among different types of surveillance as part of a categorical approach ranging from collection, through processing, through various types of usage.[2] Such approaches, while beneficial for other purposes, are too complex and thus not well-matched to address the first-order problem of disambiguating gathering from usage.

Perhaps the reason for this oversight stems from the historical tendency for the same entities within the law enforcement/intelligence community to simultaneously engage in both activities. Clearly, however, gathering is no longer limited to government entities, and thus any discussion must first separate these activities by the actors who conduct them. This Part proposes the "gathering vs. usage" distinction, and explains its applicability to the context of contemporary surveillance-harm analysis. It begins with a brief discussion of the potential harms resulting from surveillance activities.

[2] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 482–84 (2006).

1. Surveillance Harms.—Legal scholarship historically focuses on two categories of harm stemming from surveillance activities.[3] In discussing these categories, I use three terms: (1) the "gatherers"—those entities which collect, but do not necessarily use, surveillance information; (2) the "watchers"—those entities that possess or have access to surveillance information, regardless of whether they were the entities engaged in the collection; and (3) the "subjects"—those entities whose identity, characteristics, or activities are described in the surveillance information. There can be overlap among these categories, particularly in the case of historically common government surveillance.

The first category of harm involves a subject who is actually observed or who perceives they may *possibly* be observed. This category proposes that such activity or possibility will deter people from engaging in free and unfettered thought and exploration. Rather, subjects will be driven to adopt mainstream beliefs and ideals, a trend at odds with the free and open political discourse at the theoretical core of the American political system. Collectively, these harms are often described as "chilling effects," where the "chill" describes the deterrent on activities such as speech and association.[4] These harms often are considered in conjunction with a First Amendment analysis.[5]

The second category of harm focuses on the threat of or actual use of surveillance information by authorities for unlawful purposes such as arbitrary coercion, unlawful discrimination, and selective enforcement.[6] Unlike the first category, this category describes a relationship in which the subject knows that the watcher has, or can readily access, information actionable for these unlawful purposes. In other words, the subject knows the watcher can use surveillance information impermissibly, but alters their behavior or fails to do so and is directly harmed as a result.

2. Harm-Based Distinction of Gathering from Usage.—These two categories of harm historically described in privacy scholarship suggest the gathering-usage distinction. This distinction additionally derives from the logical separation between these activities—collection does not imply use (or the ability to use), and usage does not imply the ability to have chosen what to collect or to further collect.

---

[3] *See, e.g.*, Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 RUTGERS COMPUTER & TECH. L.J. 1, 2–4 (1998); Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1062–63 (2006); Stan Karas, *Enhancing the Privacy Discourse: Consumer Information Gathering as Surveillance*, 7 J. TECH. L. & POL'Y 29, 30–31 (2002); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1934–36 (2013); Solove, *supra* note 2, at 488–89; K. A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 YALE J.L. & TECH. 123, 125, 129 (2004–2005).

[4] Richards, *supra* note 2, at 1949; Solove, *supra* note 2, at 488; Taipale, *supra* note 2, at 146.

[5] Richards, *supra* note 2, at 1950; Solove, *supra* note 2, at 515–16; Taipale, *supra* note 2, at 146.

[6] Donohue, *supra* note 2, at 1192–93; Richards, *supra* note 2, at 1953–58; Solove, *supra* note 2, at 507–23; Taipale, *supra* note 2, at 150, 176.

This Section proceeds by discussing gathering and usage in turn and then concludes by linking that discussion to why the distinction is necessary.

3. Gathering Activities.—Gathering activities comprise those that acquire or generate information about an entity's identity, characteristics, or behavior. While often part of a comprehensive collection scheme with a specific usage purpose in mind,[7] not all gathering falls into this category. Gathering, for example, may simply be for administrative purposes,[8] such as toll-based wireless telephony.[9] Other gathering activities may have a more data-driven purpose—collection of consumer contact information to sell for marketing purposes, for example—but the entity doing the gathering generally does not interact with the entity using the information.[10]

In this regard, gathering is logically separable from use. The examples above illustrate how entities may gather information *usable* for surveillance, but such gathering activity has no intended relation to surveillance. This logical separation becomes important in the context of the potential harm resulting from surveillance. The relationship to the second category of harm above—unlawful threat or use of surveillance information—is obvious, as gathering activities not linked to usage lack the potential to cause this type of harm.[11]

In contrast, the first type of harm—chilling effects—illustrates precisely why gathering activities should be considered individually as a potential harm unto themselves. As discussed above, chilling effects cases focus on the potential scope of lawful activity that is deterred as a result of the potential or actual gathering of information which might later be used in an actionable way—regardless of whether

[7] Consider, for example, online behavioral advertising activities. *See, e.g.*, JOSEPH TUROW ET AL., CONTRARY TO WHAT MARKETERS SAY, AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT (2009), *available at* https://www.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf; *see also infra* Part I.B.3.

[8] "Administrative purposes" generally entails gathering ancillary to, but necessary for, the provision of a service.

[9] *In re* U.S for Historical Cell Site Data, 724 F.3d 600, 611–12, 615 (5th Cir. 2013) ("[C]ell site information is clearly a business record. The cell service provider collects and stores historical cell site data for its own business purposes, perhaps to monitor or optimize service on its network or to accurately bill its customers for the segments of its network that they use. . . . Because the magistrate judge and district court treated the data as tracking information, they applied the wrong legal standard. Using the proper framework, the SCA's authorization of § 2703(d) orders for historical cell site information if an application meets the lesser 'specific and articulable facts' standard, rather than the Fourth Amendment probable cause standard, is not per se unconstitutional.").

[10] In such cases, the dominant business model is for intermediate "clearinghouses" to match data gatherers with data users. A similar model is used in selling advertising space based on Online Behavioral Advertising information. DAVID THAW, NEHA GUPTA & ASHOK AGRAWALA, PROPOSAL FOR A "DOWN-THE-CHAIN" NOTIFICATION REQUIREMENT IN ONLINE BEHAVIORAL ADVERTISING RESEARCH AND DEVELOPMENT (2011), *available at* www.researchgate.net/publication/228419933_Proposal_for_a_Down-the-Chain_Notification_Requirement_in_Online_Behavioral_Advertising_Research_and_Development/file/9fcfd50d1df2a19cff.pdf.

[11] This is not to say that others may not use the information, but that is a separable type of harm because it is conducted by a different entity, which may be subject to different public policy balancing mechanisms.

that information is ever actually used in an actionable way.[12] In such cases, mere gathering–even if only for the most innocuous, administrative purposes—has the potential to deter lawful activity in a manner contrary to First Amendment and other basic principles of American society.

This is not to say that gathering should be prohibited. Quite the contrary, this Article takes no position on any particular case. Rather, the purpose is to illustrate why gathering activities should be analyzed distinctly from usage activities, and suggest the proper balancing mechanisms that can be applied to determine how the potential harms of those activities relate to the potential benefits. This includes considering whether the gathering is conducted by private or public entities, as each is subject to a different balancing mechanism.[13]

4. Usage Activities.—Usage activities comprise those in which information about an entity's identity, characteristics, or behavior are accessed or analyzed for the purpose of generating further information about a subject or taking action regarding a subject. These definitions are deliberately broad, and encompass activities traditionally described as "data processing," "data analysis," "data aggregation," and "data retention."[14] The core of these definitions however, is the access to or analysis of information for the purpose of taking action regarding a subject.

Following the analysis on gathering above in Section B.1., usage is logically separable from gathering in that taking action regarding a subject *on the basis of some collected information* necessarily implies access to or analysis of that information. The link to the second category of harm is obvious—if surveillance information is the basis of an unlawful action, and without that information the watcher would have been unable to take the unlawful action, the subject would not have been harmed by the surveillance. Such a harm does not *necessarily* occur—surveillance information may be used for lawful purposes, or no actions may be taken at all[15]—but its potential is sufficient to merit a distinct consideration of usage activities.

5. The Argument for the Gathering-Usage Distinction.—A harms-oriented analysis makes the strongest case for the gathering-usage distinction. The logical

[12] Reno v. Am. Civil Liberties Union, 521 U.S. 844, 872 (1997); Broadrick v. Oklahoma, 413 U.S. 601, 630 (1973) (Brennan, J., dissenting); Dombrowski v. Pfister, 380 U.S. 479, 490–91 (1965).

[13] As discussed elsewhere, first-order American political theory relies on a functioning free market (with appropriate regulatory oversight) to balance choices about private entities' surveillance activities, whereas first-order American political theory relies on the policymaking process (with appropriate judicial oversight) to balance choices about government entities' surveillance activities.

[14] All functions, for example, support the generation of further information about the subject and/or other subjects.

[15] Some scholars have argued that the potential for analysis, even if it is *not* used to generate new data or take action (i.e., the data is only viewed by the watcher) creates a chilling effect. This type of chilling effect is orthogonal to the point of whether gathering and usage should be separated as "view-only" effects would equally apply to both categories of information. *See, e.g.*, Byford, *supra* note 2, at 14.

distinctions form a foundation supporting the validity of analyzing gathering and usage separately. Other separations, however, might also be logically valid. It is the linkages between the categories of surveillance harms and the respective gathering and usage activities that demonstrate the superiority of this gathering/usage distinction.

Government surveillance historically included both gathering and usage activities, with the private sector playing a limited role. If law enforcement needed to tap a phone line, for example, the local incumbent telecommunications provider would cooperate, but law enforcement officials would initiate and conduct the surveillance. [16] Likewise, if the intelligence community wanted to track an international criminal or terrorist across national borders, they would engage government-owned and operated satellite surveillance systems, military resources, intelligence operatives, and other resources. Thus, the gathering and usage functions historically were merged, at least inasmuch as most of the entities engaged in the equation were governmental and few were private.

But times have changed. Part II of this Article discusses the increasing role the private sector plays in the gathering of data, the differing incentives private entities have for usage, and the "gaps" in the surveillance-harm calculus that result from failing to consider the role of the private sector and from conflating gathering and usage.

II. PRIVATE SURVEILLANCE

The role of private actors in government surveillance historically has been under-examined in legal scholarship on privacy. This omission is more than a mere curiosity because the mechanisms by which American society checks-and-balances the behavior of private actors are fundamentally different than those used for government activity. Now that private actors play a critical role in government surveillance, the previous answer to whether adequate protections are in place to balance the benefits and harms of surveillance must be reconsidered. This Part first explores the role of private actors in contemporary government surveillance activities. It then compares government and private actors in the context of incentives for exploitation and mechanisms to prevent abuse.

1. The Increasing Role of the Private Sector.—A quick Google search for precisely this question—the role of the private sector in government surveillance—reveals a substantial amount of media attention regarding the subject. While perhaps an odd data point from which to start, it is particularly telling, as this private sector tool for conducting research is one of the very same tools actively engaged in surveillance

[16] Note, by contrast, that in the case of "local usage directories" and long-distance calling records, the private entities maintained this data for administrative purposes. However, not all local incumbent telecommunications providers automatically retained *local* usage for administrative purposes. In certain areas, for example, law enforcement would direct individuals to enter a special code after receiving a threatening or harassing phone call, which would cause the local incumbent telecommunications provider's system to "make a note" of the call when it otherwise might not.

gathering activities. The results will vary according to context—including the time, and what information Google is able to discern about the user running the query[17]—but several commonly leading results are quite telling of the trend.[18] While it is difficult to qualify with empirical validity due to the classified nature of most historical government surveillance programs, the combination of recent judicial review of government surveillance programs[19] and recent notable alleged whistleblower disclosures[20] suggests a rapid trend toward increased reliance by the government on private actors for surveillance gathering activities.

This is not necessarily a bad thing, nor is the purpose of this Article to opine on whether the private sector should have a role in government surveillance. While harms such as those discussed in Part I certainly are risks with government surveillance activities, those activities also may produce important benefits in the areas of public health, national security, law enforcement, and economic regulation. It may well be that the private sector, particularly in the age of Big Data, is better suited than the government to be the primary actor engaged in gathering activities.

The private sector, however, is subject to a different set of balancing mechanisms to ensure that its activities are consistent with the expectations of society. Whereas government relies on the political process (with appropriate judicial oversight), the private sector relies on a healthy, functioning free market with adequate consumer choices (with appropriate regulatory oversight). Consideration of the traditional political process alone, therefore, is insufficient to ensure adequate analysis of the cost/benefit tradeoffs of contemporary surveillance.

This short Article does not discuss the details of specific examples of private sector participation in government surveillance. While adequate disclosures of certain classified programs may exist, it is not the details of the programs that are central to the thesis of this piece. Rather, this Article lays out an analytical framework suggesting that *there is* an oversight in existing literature and why that

---

[17] This fact in itself is revealing of surveillance—both gathering and usage—being conducted by the private sector for its own purposes. For more information on Google's search results, see Adam Rosenthal, *Why Google's Search Results Vary from Person to Person*, MICROARTS (June 21, 2013), http://microarts.com/launchabrand/why-googles-search-results-vary-from-person-to-person.

[18] *See generally* Human Rights Council, *The Right to Privacy in the Digital Age: Rep. of the Office of the U.N. High Commissioner for Human Rights*, U.N. Doc. A/HRC/27/37 (June 30, 2014), *available at* http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (reporting on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance); BEATRICE EDWARDS, THE RISE OF THE AMERICAN CORPORATE SECURITY STATE (2014) (discussing reasons to fear corporate surveillance); Julian Chokkattu, *U.N. Says Governments Are Increasingly Relying on Private Sector for Surveillance*, TECHCRUNCH (July 16, 2014), http://techcrunch.com/2014/07/16/u-n (discussing the U.N's fears that digital surveillance will escape governmental control); Mark Karlin, *Six Reasons to be Afraid of the Private Sector/Government Security State*, TRUTHOUT (May 16, 2014, 9:48 AM), http://truth-out.org/opinion/item/23728 (discussing privacy and surveillance by the private sector).

[19] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 948 (2012); *In re* U.S for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013); United States v. Skinner, 690 F.3d 772, 776 (6th Cir. 2012).

[20] *See generally* Ewen MacAskill & Gabriel Dance, *NSA Files: Decoded*, THE GUARDIAN (Nov. 1, 2013), http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded (examining the files uncovered by Edward Snowden).

oversight makes discussions of surveillance harms incomplete.[21]

2. Government vs. Private Cost/Benefit Analyses.—These cost/benefit tradeoffs form the core of the central argument of this Article—that existing discussions of the surveillance-harm calculus are incomplete. The premise for this claim is that public and private sector entities have different incentives to engage in surveillance and that they are subject to different balancing mechanisms to weigh those cost/benefit tradeoffs. This Section explores these differences and highlights the incomplete aspects of a surveillance-harm discussion that under-appreciates the private sector's role in government surveillance.

3. Government Surveillance (Incentives and Balancing Mechanisms).—Government incentives for surveillance primarily stem from public services that require or can be improved by better information about individual or organizational attributes and conduct. Classic examples include public health, national security, law enforcement, and economic policy. Public health is a particularly useful starting point because the tradeoff is less politically controversial than national security or law enforcement—in the modern era, gathering information about the travel habits of individuals exposed to a deadly virus is comparatively less controversial than are terrorism watch lists. Such gathering is limited in scope, the usage of the information is limited in scope, the gathering generally is done openly, and the opportunities for abuse are comparatively limited because the information is subject to substantial public scrutiny. Such gathering is not without controversy, however, as certain transmission vectors—such as intimate contact in the case of sexually transmitted infections—may include far more sensitive information than people are comfortable being compelled to share. Additionally, the potential for abuse of such information generally is greater than with less intimate information such as travel habits.

National security and law enforcement contexts produce comparatively high levels of debate. Since September 11, 2001, government anti-terrorism surveillance activity has increased dramatically, presenting the challenge of balancing the prevention of potentially massive loss-of-life with the protection civil liberties.[22] Contrary to public health, the incentives for law enforcement and intelligence agencies are to gather as much information as possible and to make the most comprehensive use of it. These goals are aligned with the prevention and prosecution of terrorist and other criminal activities. Also in contrast to public health, such surveillance generally is conducted in secret both to preserve the integrity of the investigative process and to increase the likelihood of success in detecting unlawful activities that actors seek to conceal. This secrecy and the nature and scope of the information collected make it ripe for abuse because reduced

[21] The particulars of the programs are more appropriate for the planned second piece in this series, which will include an empirical analysis of those programs, private sector programs, and a comparison of the balancing mechanisms in place to address surveillance cost/benefit tradeoffs for each activity.

[22] *See, e.g.*, 50 U.S.C. § 1861 (2012).

transparency likewise reduces the probability of abuse being detected, thus reducing one important deterrent against abuse.

This brief analysis highlights two key aspects of government surveillance activities. First, that the policymaking process is the mechanism for balancing privacy interests and public goals. The elected legislatures and executive(s) of the states and the federal government are responsible for directing and overseeing the activities of these organizations with appropriate additional oversight by the judicial system. Second, that the primary incentives are public ones, such as the protection of public health and prevention of criminal activity, not private ones, such as profit-making. While the nature of these incentives by no means obviates the need for oversight and balancing mechanisms to protect against surveillance harms, the *inherent goals* are at least aligned with valid *public* interests, as different from private sector entities.

4. *Private Surveillance (Incentives and Balancing Mechanisms).*—Private incentives for surveillance stem primarily from instrumental incentives and direct-profit incentives. Instrumental incentives include surveillance activities that a private entity must conduct in order to deliver its primary good or service. Direct-profit incentives include surveillance activities that a private entity conducts for the value of the data gathered itself, whether directly or for enhancing the value of other products or services.

An example of an instrumental incentive is the use of wireless telephone records as to a subscriber's location, phone numbers called, and time and duration of calls. All of this information is necessary in order to create and maintain accurate billing records and must be gathered as an instrumental matter regardless of whether the carrier intends on otherwise monetizing it. An example of a direct-profit incentive, by contrast, is the collection of a user's web browsing habits across multiple websites by an online behavioral advertising network. Although the delivery of targeted advertising does not, as a mathematical matter, strictly *require* collecting information about a user's web browsing habits, the industry asserts that such gathering and usage greatly enhances the accuracy of the targeting and thus increases its effective value to potential marketers. [23]

While these two incentives are different in certain respects, they share a common important distinction from government surveillance activities—both have a primary purpose of supporting the profit-making enterprise of a private organization. Neither has a public service as its primary goal. While it is true that many private companies are filling historically public roles, particularly in recent years, the structure of corporate law creates a fiduciary duty for profit-making

[23] *See* THAW, GUPTA & AGRAWALA , *supra* note 10, at 1; *see also Understanding Online Advertising: Frequently Asked Questions*, NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/faq (last visited Jan 26, 2014).

enterprises to deliver optimal profit to their shareholders.[24]

The mechanism for balancing the beneficial behaviors of private organizations—in this case, defined as profit-making—against potential harms is a free, functioning healthy marketplace with consumer choice and appropriate regulatory supervision. Similar to the incentives, this mechanism is also very different from that for balancing government-beneficial activities against potential harms.

Whereas a functioning legislative and executive policymaking balancing mechanism has certain requisite elements, such as universal suffrage and other elements of adequate participation in the political process, a functioning free market as a balancing mechanism has fundamentally different requisite elements. Two of these elements are relevant to consideration of the surveillance-harm calculus. First, the market must be functioning properly—that is, consumers must be able to express their preferences through purchase choices. When other variables, such as switching costs,[25] obstruct that preference expression, the market no longer performs a balancing function because organizations are not incentivized to alter their products based on consumer preferences if it is otherwise too difficult for consumers to switch to an alternative (or if one does not exist because barriers to entry are too high). Second, even assuming consumers are able to express

[24] *See, e.g.*, Dodge v. Ford Motor Co., 170 N.W. 668, 684 (Mich. 1919) ("A business corporation is organized and carried on primarily for the profit of the stockholders. The powers of the directors are to be employed for that end. The discretion of directors is to be exercised in the choice of means to attain that end, and does not extend to a change in the end itself, to the reduction of profits, or to the nondistribution of profits among stockholders in order to devote them to other purposes."). While *Dodge* deals primarily with Michigan law, this is often considered the leading case on the subject across jurisdictions. *See* Stephen Bainbridge, *Case Law on the Fiduciary Duty of Directors to Maximize the Wealth of Corporate Shareholders*, PROFESSORBAINBRIDGE.COM (May 5, 2012, 12:18 PM), http://www.professorbainbridge.com/professorbainbridgecom/2012/05/case-law-on-the-fiduciary-duty-of-directors-to-maximize-the-wealth-of-corporate-shareholders.html.

[25] Jacques Crémer & Gary Biglaiser, *Switching Costs and Network Effects in Competition Policy, in* RECENT ADVANCES IN THE ANALYSIS OF COMPETITION POLICY AND REGULATION 13, 13 (Joseph E. Harrington Jr. & Yannis Katsoulacos, eds., 2012) ("Using a social networking site that does not have any other users does not increase one's utility. . . . Consumers will hesitate to 'leave' an incumbent, even to migrate to an entrant which offers lower prices and/or better quality, as they fear that they will lose the benefits . . . ."); Juan Pablo Maicas et. al., *The Role of (Personal) Network Effects and Switching Costs in Determining Mobile Users' Choice*, 24 J. INFO. TECH. 160, 160 (2009), *available at* http://www.palgrave-journals.com/jit/journal/v24/n2/abs/jit200835a.html ("[P]ersonal network effects and switching costs play a key role in determining mobile users' choice: the probability that a customer selects a mobile phone company increases with the number of members of her social network already subscribed to that firm, and switching costs are significantly present in the mobile phone market making switching providers costly."); Justus Haucap & Ulrich Heimeshoff, *Google, Facebook, Amazon, eBay: Is the Internet Driving Competition or Market Monopolization?* 7 (DICE Discussion Paper No. 83, 2013), *available at* www.econstor.eu/bitstream/10419/68229/1/73435858X.pdf ("[C]osts between social networks such as *Facebook* are generally much higher because . . . the number of users is a very important factor for users' utility."); Irina Suleymanova & Christian Wey, *Bertrand Competition in Markets with Network Effects and Switching Costs* 2 (DICE Discussion Paper No. 30, 2011), *available at* www.econstor.eu/bitstream/10419/48679/1/665466420.pdf; Ming-Chien Lin, Investigate the Impact of Inertia Formation on The New System Acceptance-An Empirical Study of Social Network Sites (July 16, 2013) (unpublished Master's thesis), *available at* http://etd.lib.nsysu.edu.tw/ETD-db/ETD-search/view_etd?URN=etd-0616113-215318.

preferences about a product at all, other variables such as price, functionality, and "The Next Big Thing"[26] tend to dominate consumer decisions over functions such as privacy[27] and security.[28]

It is worth noting that in recent months, companies such as Apple,[29] Microsoft,[30] and Google[31] have responded to the trend in government requests for information by offering products designed to allow users to encrypt their own mobile devices in a manner these vendors claim will lock the vendors themselves out of the devices. Although the existence of these products appears to counter the proposition that "consumers are unable to express privacy preferences," a few things are worth noting regarding such assertions.

First, these technologies have existed for many years, and in fact, in many cases the advertised "change" is simply to enable those features to be active by default as opposed to lay users making potentially confusing changes to technical settings in their devices.[32] Thus, the original preference expressed by the market was less likely to be consumers responding to government surveillance revelations (since those revelations had not yet occurred) and was more likely to be a response to demands by large organizational clients to provide encryption for data security compliance purposes.[33] Second, responding to government requests for surveillance information is an expensive, time-consuming process for service providers. By locking themselves out of access to information, they can substantially reduce their own costs. It may well be the case that this is one example where public and private interests *happen* to align,[34] however, in the context of a balancing mechanism to ensure privacy and surveillance concerns are properly considered, happenstance is not sufficient to protect against potential harms.

---

[26] Samsung, *Samsung Galaxy S II (The Next Big Thing) Commercial*, YOUTUBE (Nov. 22, 2011) http://www.youtube.com/watch?v=GWnunavN4bQ.

[27] James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 1–2 (2005).

[28] Ross Anderson & Tyler Moore, *The Economics of Information Security: A Survey and Open Questions*, 314 SCIENCE 610, 611 (2006) ("Consumers generally reward vendors for adding features, for being first to market, or for being dominant in an existing market . . . . These motivations clash with the task of writing more secure software, which requires time-consuming testing and a focus on simplicity.").

[29] Tom Gillis, *Apple's iOS 8 Lets Users Just "Trust the Math"*, FORBES (Oct. 14, 2014, 2:50 PM), http://www.forbes.com/sites/tomgillis/2014/10/14/apples-ios-8-lets-users-just-trust-the-math.

[30] Lou Shipley, *Why the Future of Digital Security Is Open*, TECHCRUNCH (Oct. 17, 2014), http://www.msn.com/en-us/news/technology/why-the-future-of-digital-security-is-open/ar-BB9uSk2.

[31] Danny Yadron & Rolfe Winkler, *Google to Encrypt Phone Data in Android*, WALL ST. J.: DIGITS (Sept. 18, 2014, 7:28 PM), http://blogs.wsj.com/digits/2014/09/18/google-to-encrypt-phone-data-in-android.

[32] Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids.

[33] David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 321 (2014) ("[T]he security investment is moved essentially to crypto. Just encrypt as much as you can. Whatever it takes, just encrypt it. If it moves, encrypt it. If it stays there, encrypt it.).

[34] A useful circumstance that I discuss the benefits of elsewhere. *See* David Thaw, *Enlightened Regulatory Capture*, 89 Wash. L. Rev. 329, 332–33 (2014).

CONCLUSION

The result is a circumstance in which the discussion about how to balance the public benefits of surveillance against the potential harms is undoubtedly insufficient and does not consider all of the relevant factors. This Article does not argue for or against government surveillance—rather, it focuses on the fact that whatever conclusion is reached, if that conclusion fails to separate gathering from usage activities in analysis of surveillance, or fails to include the role of the private sector, that discussion is necessarily incomplete. It is incomplete in the former instance because it fails to recognize the different purposes and resultant harms associated with each category of surveillance activity. It is incomplete in the latter instance because it assumes that one type of balancing mechanism—the policymaking process for government oversight—will be adequate to "spill-over" onto the behaviors of the private sector. This is an assumption with far too much risk given the potential harms at stake. Therefore, a proper analysis requires empirical investigation of the categories of activities and of the actual and potential harms among different types of surveillance activities.[35]

[35] In the next piece in this series, I plan to construct a matrix of these activities and the applicable oversight mechanisms and use the framework from this Article to describe what are the likely harms of each type of surveillance program and what a "complete" discussion of each cost/benefit analysis would require.