UNILATERAL INVASIONS OF PRIVACY

*Roger Allan Ford**

ABSTRACT

Most people seem to agree that individuals have too little privacy, and most proposals to address that problem focus on ways to give those users more information about, and more control over, how information about them is used. Yet in nearly all cases, information subjects are not the parties who make decisions about how information is collected, used, and disseminated; instead, outsiders make unilateral decisions to collect, use, and disseminate information about others. These potential privacy invaders, acting without input from information subjects, are the parties to whom proposals to protect privacy must be directed.

This Article develops a theory of unilateral invasions of privacy rooted in the incentives of potential outside invaders. It first briefly describes the different kinds of information flows that can result in losses of privacy and the private costs and benefits to the participants in these information flows. It argues that in many cases the relevant costs and benefits are those of an outsider deciding whether certain information flows occur. These outside invaders are more likely to act when their own private costs and benefits make particular information flows worthwhile, regardless of the effects on information subjects or on social welfare. And potential privacy invaders are quite sensitive to changes in these costs and benefits, unlike information subjects, for whom transaction costs can overwhelm incentives to make information more or less private.

The Article then turns to privacy regulation, arguing that this unilateral-invasion theory sheds light on how effective privacy regulations should be designed. Effective regulations are those that help match the costs and benefits faced by a potential privacy invader with the costs and benefits to society of a given information flow. Law can help do so by raising or lowering the

* Assistant Professor of Law, University of New Hampshire School of Law; Faculty Fellow, Franklin Pierce Center for Intellectual Property. For helpful comments and conversations, I am indebted to Alex Boni-Saenz, Andrew Selbst, Angela Kuhnen, Avner Levin, Catherine Crump, Helen Nissenbaum, Ira Rubinstein, Jennifer Berk, Joseph Lorenzo Hall, Katherine Strandburg, Lior Strahilevitz, Orin Kerr, Paul Gowder, Saul Levmore, Victoria Schwartz, and participants at the sixth Privacy Law Scholars Conference at the University of California Berkeley, the NYU Privacy Research Group, and the Consumer Federation of America's Consumer Dialogue Retreat. This Article originated in work conducted during my time as a Microsoft Research Fellow at the Information Law Institute, New York University School of Law, and was supported in part by generous grants from Microsoft Corporation and the Air Force Office of Scientific Research's Multidisciplinary University Research Initiative (grant no. ONR BAA 07-036).

costs or benefits of a privacy invasion, but only after taking account of other costs and benefits faced by the potential privacy invader.

INTRODUCTION

Shortly before Thanksgiving in 2011, shopping mall operator Forest City Commercial Management announced that it would begin tracking shoppers' movements in two of their malls, using the signals from cell phones to trace individual paths from store to store.[1] The malls would use a technology called FootPath that, as its maker, Path Intelligence, explained, could help an operator understand shoppers' behavior and use this information to make "[d]ecisions that optimize tenant performance, protect and drive lease values, maximize operating income, and ultimately, drive asset value."[2]

Tracking shoppers' movements was not a new phenomenon; malls and other retailers have long looked to see where customers linger, what areas they avoid, and what stores attract like-minded shoppers.[3] Nor was the FootPath system itself new; even before the Thanksgiving announcement, the Path Intelligence technology was used by malls in Australia and the United Kingdom.[4] Yet Forest City's tracking lasted just one day before the backlash from regulators and others raising privacy concerns.[5] In letters to Path Intel-

1 Annalyn Censky, *Malls Track Shoppers' Cell Phones on Black Friday*, CNN (Nov. 22, 2011, 11:48 AM), http://money.cnn.com/2011/11/22/technology/malls_track_cell_phones_black_friday/.

2 *See ICSC Signs Global Agreement with Shopper Locations Analytics Provider Path Intelligence*, ICSC, (Mar. 23, 2015), http://www.icsc.org/press/icsc-signs-global-agreement-with-shopper-location-analytics-provider-path-i. While this Article was in the publication process, Path Intelligence ceased operations and went into administration, the United Kingdom's rough equivalent of bankruptcy reorganization.

3 *E.g.*, Method and Sys. for Automatic Analysis of the Trip of People in a Retail Space Using Multiple Cameras, U.S. Patent No. 8,098,888 (filed Jan. 28, 2008) (issued Jan. 17, 2012); Sys. and Method for Customer Behavior Movement Frequency Prediction in a Store, U.S. Patent No. 7,778,863 (filed Sept. 13, 2005) (issued Aug. 17, 2010); Customer Activity Monitor, U.S. Patent No. 5,250,941 (filed Aug. 9, 1991) (issued Oct. 5, 1993); Jeffrey S. Larson et al., *An Exploratory Look at Supermarket Shopping Paths*, 22 INT'L J. RES. MARKETING 395 (2005); Censky, *supra* note 1.

4 *Shopping Centers Track Customers Via Cell Phone Signals*, SLASHDOT (May 18, 2008, 2:56 PM), http://yro.slashdot.org/story/08/05/18/1838222/shopping-centers-%20track-customers-via-cell-phone-signals; Kylie Collier, *'Creepy' Path Intelligence Retail Technology Tracks Shoppers*, NEWS.COM.AU (Oct. 14, 2011, 8:24 AM), http://www.news.com.au/finance/money/creepy-retail-technology-tracks-shoppers/story-e6frfmci-1226166413071; Steven Morris, *Shopping Centre Tracking System Condemned by Civil Rights Campaigners*, GUARDIAN (Jan. 4, 2012, 3:19 PM), http://www.theguardian.com/business/2012/jan/04/shopping-centre-tracking-system-condemned.

5 *See, e.g.*, Sean Gallagher, *We're Watching: Malls Track Shopper's* [sic] *Cell Phone Signals to Gather Marketing Data*, ARS TECHNICA (Nov. 25, 2011, 4:15 PM), http://arstechnica.com/business/2011/11/were-watching-malls-track-shoppers-cell-phone-signals-to-gather-marketing-data/ ("There's just one problem with this type of detailed tracking: it's technically illegal, according to Mark Rasch, the director of cybersecurity at CSC."); Press Release, Senator Charles E. Schumer, Schumer Reveals: This Holiday Season, New Technology Could be Tracking Shoppers' Movements in Shopping Centers Through Their Cell

ligence and to the Federal Trade Commission, Senator Charles Schumer objected that shoppers would be tracked without their consent and could only opt out by turning off their cell phones or avoiding shopping malls, burdens he argued were unreasonable.[6] Faced with this scrutiny, Forest City pulled the plug on the automated tracking.[7] So rather than tracking shoppers via cell phone, the Forest City malls will have to adopt more costly means of tracking shoppers or forswear the benefits that FootPath promised.[8]

The FootPath story is typical of a recurring scenario in information-privacy law: a new practice that seems creepy and invasive, even though it results in many of the same information flows that existed before the practice. Privacy law has struggled with such developments. Under the dominant legal view, there is no privacy problem with what Forest City aimed to do. The system collected information about shoppers' visible movements in a public place—information that seems public, in some sense, and can freely be collected by any number of observers. The information did not concern shoppers' sensitive, personal, or intimate lives; none of it was inherently "private," in that sense. Yet shoppers, and Senator Schumer, had an immediate and visceral reaction that the system would compromise their privacy. It mattered to them that information about more shoppers would be collected and used, even if there was nothing especially sensitive about the specific information collected.

This scenario also occurs in Fourth Amendment law. For decades, it was axiomatic that a criminal defendant cannot expect privacy in his or her activities in public.[9] As the Court explained in *United States v. Knotts*, such activities are inherently and inevitably revealed to the world:

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] traveled over the public streets he volunta-

---

Phones; Calls For Mandatory Opt-in Before Retailers Are Allowed to Track Shoppers' Movements (Nov. 28, 2011) [hereinafter Press Release].

6 Press Release, *supra* note 5.

7 Sean Gallagher, *Mall Owners Pull Plug on Cellular Tracking (For Now)*, WIRED (Nov. 29, 2011, 11:11 AM), http://www.wired.com/epicenter/2011/11/mall-pull-plug-cell-tracking/.

8 Or they will just have to wait until technologies like FootPath's are no longer considered novel and threatening. Indeed, in the time since Forest City killed its plans, several other companies have announced or begun using systems that do much the same thing. *See, e.g.*, Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES (July 14, 2013), http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html; Brian Fung, *How Stores Use Your Phone's WiFi to Track Your Shopping Habits*, WASH. POST (Oct. 19, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/10/19/how-stores-use-your-phones-wifi-to-track-your-shopping-habits/; Declan McCullagh, *Euclid Downplays Privacy Concerns About Wi-Fi Tracking*, CNET (May 16, 2012, 5:36 PM), http://news.cnet.com/%208301-1009_3-57435911-83/.

9 *See* United States v. Knotts, 460 U.S. 276, 281–82 (1983); Hester v. United States, 265 U.S. 57, 58 (1924) (affirming conviction when "[t]he defendant's own acts, and those of his associates, disclosed [to the public] the jug[,] the jar and the bottle" that showed illegal concealment of distilled spirits).

> rily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.[10]

Since a defendant voluntarily revealed his movements to the world simply by moving around in public, an officer gathering that public information did not conduct a "search" for purposes of the Fourth Amendment.

Yet in 2012, the Court unanimously reversed course, concluding in *United States v. Jones* that using a GPS device to monitor a defendant's movements in public is a search for which a police officer might have to obtain a warrant.[11] The Court divided on its reasoning, but five Justices recognized that GPS monitoring presented new and unique privacy concerns even if the devices only collected information that could otherwise be obtained by conventional police techniques. By removing obstacles to such full-time surveillance, the Justices reasoned, GPS technologies made it likely that many more defendants would be tracked, a distinction that mattered for privacy.[12]

Criminal defendants are hardly alone: more information is being collected, used, and disseminated today than at any point in history, a trend that shows no signs of slowing. Several factors have contributed to this trend, including changes in laws, social norms, and incentives. The main driver, however, is evolving technology, which has made it easier and cheaper for people to collect, use, and disseminate information about others. It's not inevitable that technology would have this effect; individual technology changes can make information flows more or less common. Yet the net effect has been a striking increase in the amount of information collected, used, and disseminated to others.

The dominant response to this increase in information flows has differed between the private and public sectors. In the public sector, courts and legislatures have used the Fourth Amendment and new statutes to limit the ability of law-enforcement agencies to collect and use information.[13] These laws have generally worked by regulating the outsider—the entity collecting, using, or disseminating information about someone else—rather than the information subject. In the private sector, however, the focus has been different. Most responses to privacy concerns in the private sector have aimed to inform information subjects about how personal information is used and control over that use. Thus, Senator Schumer urged Path Intelligence "to obtain the explicit consent of shoppers' [sic] through an opt-in policy in

10 *Knotts*, 460 U.S. at 281–82.

11 132 S. Ct. 945, 953 (2012).

12 *Jones*, 132 S. Ct. at 955–57 (Sotomayor, J., concurring); *id.* at 963–64 (Alito, J., concurring in the judgment).

13 *See, e.g.*, *Jones*, 132 S. Ct. 945; Kyllo v. United States, 533 U.S. 27 (2001); *see also* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

order to protect their privacy" before deploying the FootPath system.[14] And in numerous enforcement actions against private companies that failed to protect consumers' privacy, government agencies have focused on failures of transparency and control, rather than targeting the underlying behavior. The dominant response, then, has been to focus on the information subject as the relevant decisionmaker, rather than on the outsider collecting, using, or disseminating information.[15]

This focus on information subjects is puzzling because in many cases, information flows happen without the consent, or even the knowledge, of information subjects. Instead, often an outsider like Path Intelligence is the sole decisionmaker determining whether the information flow happens in the first instance. Although these regulatory responses can be thought of as efforts to ensure information subjects also participate in the decision that an information flow goes forward, they usually do so indirectly at best, and they have had little effect in preventing unwanted information flows.

This Article examines the dynamic seen in the FootPath and *Jones* cases, and in countless other contexts, seeking to understand why more and more information is being collected, used, and disseminated, even as shoppers, Supreme Court Justices, and others find this trend so troublesome. The core contention is that there is a category of information flows for which the party that determines whether the information flow occurs—the decisionmaker—is someone other than the information subject. Such information flows, which I call unilateral invasions, occur when the interests of the potential invader dictate, rather than when the interests of society or the information subject would dictate.[16] This creates a basic asymmetry between the factors that influence how much privacy any given individual has and the benefits of that level of privacy: although privacy offers benefits both to information subjects and to society as a whole, it is often individuals other than the information subjects who determine the amount of privacy that exists. Since these outsiders act according to their own incentives, ignoring or discounting the effects on information subjects and society as a whole, they systematically underprotect privacy. This situation has been exacerbated by evolving technologies, laws, norms, and incentives, which have increased the incentives to invade privacy.

This Article proceeds as follows. Part I provides background, discussing various factors that dictate whether an information flow will happen or not.

---

14 Press Release, *supra* note 5.

15 *See, e.g.*, Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013) (labeling this dominant approach "privacy self-management").

16 By calling them unilateral invasions, I do not mean to suggest that the subject of the information necessarily objects to the invader's action; he or she may welcome it or even want it to occur. But the critical point is that information flows are often initiated by outsiders, acting without the information subject's initiative, cooperation, consent, or even knowledge.

Part II develops a descriptive account of privacy based on these factors. Most privacy law and literature is focused on protecting information that is considered secret, sensitive, or intimate as "private." Yet people can react as strongly to invasions that involve no secret, sensitive, or intimate information—indeed, that involve information that is otherwise freely available to the public—as the FootPath and *Jones* cases show. This Part first argues that many information flows, including the ones at issue in the most serious privacy problems, happen because of unilateral decisions by outsiders, not information subjects, and thus can be described as unilateral invasions. It then discusses two models to predict when unilateral invasions will occur. Under a rational-choice model, a unilateral invasion will occur when the outsider's private benefits exceed the private costs of the invasion, regardless of the social value of the information flow. That model, however, fails to account for various sources of uncertainty that render the rational-choice model an unrealistic account of privacy in the real world. A stochastic-choice model, like a rational-choice model, considers the private costs and benefits of information flows, while also accounting for these uncertainties. These descriptive approaches, I argue, both better reflect people's real-world instincts about where information falls on a spectrum between "public" and "private," and are more useful in a variety of legal contexts.

Finally, Part III discusses how unilateral invasions can help provide a framework for regulating privacy. The goal of privacy regulation should be to help ensure that the levels of privacy people experience in the real world—i.e., where information falls on the spectrum from "public" to "private"—match some normative view of ideal levels of privacy. A key consequence of the unilateral-invasion theory, then, is that regulations can work most effectively by adjusting the private costs and benefits of the decisionmaker, i.e., the potential unilateral invader, rather than trying to give information subjects greater knowledge or control over how information about them is collected, used, and disseminated. If these costs and benefits lead to too much information being made public, then law can respond by increasing the costs, or reducing the benefits, of an invasion. Moreover, law can adapt dynamically to changes in these costs and benefits due to changing technologies, norms, or incentives. Indeed, this is exactly what the Court did in *Jones*, and what Senator Schumer threatened to do in the shopping mall case.

I. The Costs and Benefits of Information Flows

This Part discusses the factors that make information flows more or less likely to occur. At its most basic, information privacy is the study of information flows, or the ways in which information (say, about a person) moves

through society.[17] In this Article I focus on three broad categories of information flows: the collection, use, and dissemination of information.[18]

These three types of information flows share a key feature: in each type, an outsider can increase his, her, or its knowledge about an information subject, potentially leading to a privacy problem.[19] For instance, information collection includes surveillance, online tracking, and interrogation, all activities directed to obtaining information about someone.[20] Likewise, information dissemination can include disclosure, breach of confidentiality, and appropriation, all activities directed to providing information about someone to others.[21]

Information use is the trickiest category. While many uses of information are benign—a magazine could not deliver issues to its subscribers without knowing their names and addresses—others can have effects similar to collection and dissemination. An information aggregator, for instance, can combine different sources of information about a person to infer new facts about that person—potentially highly revealing facts, even from seemingly innocuous information.[22] Banks and credit-card companies have made extensive use of this process, even going so far as to infer that shoppers who

17 *E.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT 2 (2010) ("What people care most about is not simply *restricting* the flow of information but ensuring that it flows *appropriately*.").

18 *See generally id.* at 11, 21–64 (discussing "tracking and monitoring," "aggregation and analysis," and "dissemination and publication"); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 106–61 (2008) (discussing "information collection," "information processing," and "information dissemination"); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1373, 1417 (2000) (discussing the "collection, use, and exchange" and the "collection, processing, and exchange" of information). Note that I am not focusing on other issues, like sexual privacy, harassment, freedom of association, or nuisances, that are sometimes thought of as questions of privacy, but that do not involve information. *See, e.g.*, Roe v. Wade, 410 U.S. 113, 152–56 (1973); Griswold v. Connecticut, 381 U.S. 479, 483–86 (1965); N.A.A.C.P. v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958); SOLOVE, *supra*, at 161–70; Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980); *cf.* Lawrence v. Texas, 539 U.S. 558 (2003) (focusing on whether the petitioners had a liberty interest, rather than a privacy interest, in private sexual activities).

19 By "outsider," I mean any participant in the information flow other than the information subject, that is, the person to whom the information relates. So, for instance, when police arrest a suspect and process him or her by taking a mug shot and fingerprints, the arrestee is the information subject, and potential outsiders include the police who collect the mug shot and fingerprints, the lab tech who compares the fingerprints to prints collected at a crime scene and uploads the fingerprints to a fingerprint database, the witness who reviews the mug shot as part of a photo line up, and the investigators in other cases who make later use of the mug shot and fingerprints. Sometimes the outsider will be a party to an information flow, such as when a patient discusses his or her feelings with a therapist; sometimes the outsider will be a third party to the information flow, such as when the government intercepts an email between an information subject and someone else.

20 *See* NISSENBAUM, *supra* note 17, at 21–35; SOLOVE, *supra* note 18, at 106–17.

21 *See* NISSENBAUM, *supra* note 17, at 51–64; SOLOVE, *supra* note 18, at 136–61.

22 *See* SOLOVE, *supra* note 18, at 117–21.

put certain purchases on their credit cards, like generic car oil or marriage counseling, are larger credit risks than those who buy premium brands or home-improvement tools.[23] Personal identification, such as when police identify a suspect from DNA, is another example, since linking particular pieces of information to specific individuals can have a similar effect to information collection or dissemination. And this process can take seemingly innocuous information and use it to infer strikingly sensitive information. Device fingerprinting, for example, takes minor technical details from a device—say, a web browser's user-agent string, plugins, and time zone, or a camera's dead pixels and lens scratches—to uniquely identify a user; this can link up seemingly unrelated activity, like someone's shopping history and their porn habits.[24] This kind of inference can make it difficult or impossible for people to act anonymously or pseudonymously, which can make it hard to experiment and progress in self-development.[25]

In addition to classifying information flows as involving the collection, use, or dissemination of information, we can also focus on the participants involved in the information flow. For any information flow involving information about a person, there will necessarily be an information subject. In most cases there will also be others collecting, using, disseminating, or receiving the information, or otherwise facilitating the information flow.[26] For information collection, the relevant outsider is usually the collector; examples include a police officer following a suspect and an advertising company

23 *See* Charles Duhigg, *What Does Your Credit-Card Company Know About You?*, N.Y. TIMES MAG. (May 12, 2009), http://www.nytimes.com/2009/05/17/magazine/17credit-t.html; Stacey Vanek Smith, *Credit Card Companies Are Watching You*, MARKETPLACE (July 8, 2009, 4:28 PM), http://www.marketplace.org/topics/business/borrowers/credit-card-companies-are-watching-you.

24 *See, e.g.*, U.S. Patent No. 8,965,041 (filed July 16, 2014) (issued Feb. 24, 2015) (describing and claiming, in a patent assigned to Facebook, a system to determine unique camera signatures and associate individual cameras with users); U.S. Patent No. 8,818,022 (filed June 13, 2013) (issued Aug. 26, 2014) (same); *Panopticlick: How Unique—and Trackable—Is Your Browser?*, ELEC. FRONTIER FOUND., https://panopticlick.eff.org/ (last visited Jan. 27, 2016).

25 *See* SOLOVE, *supra* note 18, at 121–25.

26 *See, e.g.*, NISSENBAUM, *supra* note 17, at 140–47 (discussing norms governing the flow of information from a sender to a recipient). In rare circumstances, the information subject may be the only relevant party. A good example is the case of personal analytics, when someone tracks data about his or her own life. *E.g.*, Kashmir Hill, *Adventures in Self-Surveillance: Fitbit, Tracking My Movement and Sleep*, FORBES (Feb. 25, 2011, 12:07 PM), http://www.forbes.com/sites/kashmirhill/2011/02/25/adventures-in-self-surveillance-fitbit-tracking-my-movement-and-sleep/ (describing the Fitbit, a small device that attaches to clothing and tracks the wearer's movements and activity throughout the day); Stephen Wolfram, *The Personal Analytics of My Life*, STEPHEN WOLFRAM BLOG (Mar. 8, 2012), http://blog.stephenwolfram.com/2012/03/the-personal-analytics-of-my-life/ (reporting data from more than two decades of self tracking); *see also* QUANTIFIED SELF, http://quantifiedself.com/ (last visited Dec. 1, 2015) (blog devoted to "self knowledge through numbers"). For the most part, we can set these cases aside, both because they seem relatively rare and because they do not present the same privacy difficulties as other kinds of information flows.

using cookies to track a user's web-browsing behavior. For information dissemination, outsiders can include the party disseminating the information and any parties receiving the information. Examples of dissemination include a magazine publishing information about a celebrity and a database company making available public records about a taxpayer. And when information about a subject is used, the relevant outsider is typically the user. Uses of information take many forms, but the common feature is that the outsider takes information about others and processes it in a way that allows it to make inferences about, or affect the interests of, the information subjects. Well-known examples include financial institutions that process information to make credit decisions and political campaigns that target likely voters based on information in consumer databases.[27] But not all uses involve large databases of personal information; Joe Klein was famously unmasked as the anonymous author of the novel *Primary Colors* based on handwriting analysis and comparisons between the novel and his other writings.[28] Such targeted uses of information can likewise present privacy problems. Regardless, all of these information flows affect their various participants—the information subjects; outside collectors, disseminators, or users; and any outside recipients—in various ways, and those effects will, in many cases, determine whether or not the information flow occurs.

These effects are also dynamic: there is widespread recognition that evolving technology has made certain kinds of information flows more common, or even possible for the first time. The instances of location tracking recounted in the introduction provide one example, but others are common. Widespread access to public and commercial databases has made re-identification of "anonymized" records possible;[29] facial-recognition software has

27 *See* SASHA ISSENBERG, THE VICTORY LAB (2012); Colin Delany, *The Nuts and Bolts of Obama's Data-Driven Campaign*, CAMPAIGNS & ELECTIONS, Jan.–Feb. 2013, at 16–17; Craig Timberg & Amy Gardner, *Democrats Push to Redeploy Obama's Voter Database*, WASH. POST (Nov. 20, 2012), https://www.washingtonpost.com/business/economy/democrats-push-to-redeploy-obamas-voter-database/2012/11/20/d14793a4-2e83-11e2-89d4-040c9330702a_story.html; supra note 23 and accompanying text.

28 *E.g.*, Doreen Carvajal, *Columnist's Mea Culpa: I'm Anonymous*, N.Y. TIMES (July 18, 1996), http://www.nytimes.com/1996/07/18/us/columnist-s-mea-culpa-i-m-anonymous.html.

29 *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1841–45 (2011); Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117 (2013); Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1 (2011). There is also a substantial computer-science literature on identification of individuals using purportedly anonymous data. *See, e.g.*, Yves-Alexandre de Montjoye et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 347 SCIENCE 536 (2015); Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, *in* PROCEEDINGS OF THE 2008 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 111–125 (2008); Latanya Sweeney, k-*Anonymity: A Model For Protecting Privacy*, 10 INT'L J. ON UNCERTAINTY, FUZZINESS & KNOWLEDGE-BASED SYS. 557 (2002); Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* (Carnegie Mellon, Data Privacy Working Paper No. 3, 2000); *see also*

made it possible to find criminals hiding in crowds;[30] increased computational power has made it possible to decode encrypted communications;[31] and even information flows as simple as text messaging and instant messaging did not exist until technology made them possible.

Technology has made these information flows more common because it has lowered their cost or increased their benefits, and thus made it easier for decisionmakers to undertake the information flows. Yet technology is not the only source of changed costs; numerous other factors affect decisionmakers' relative costs and benefits. And the examples recounted in the introduction show the importance of this analysis. In the shopping mall case, the malls took a form of analysis retailers have long performed—tracking shoppers' footpaths—and automated it. This meant they could collect the exact same information—with presumably the same value—at a substantially lower cost. Since costs were lower, but benefits were presumably unaffected, it was suddenly worthwhile to perform this sort of analysis on a wider scale. The same was true in the case of GPS surveillance. The radio transmitters at issue in *Knotts* could only be picked up within a limited range, so police still had to follow the target car around the clock, limiting the surveillance to a few days.[32] The GPS device in *Jones*, however, recorded its own movements for a month; all the police had to do was place it on the suspect's car and retrieve it a month later.[33] And even that may no longer be required: police have gained access to built-in GPS units included in some modern cars,[34] and

Ohm, *supra*, at 1705 nn.4 & 5 (citing sources); Schwartz & Solove, *supra*, at 1842–43 nn.147–56 (same).

30 *E.g.*, Vickie Chachere, *Biometrics Used to Detect Criminals at Super Bowl*, ABC NEWS (Feb. 13, 2001), http://abcnews.go.com/Technology/story?id=98871.

31 *E.g.*, Christopher Soghoian, The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance 16 (Aug. 2012) (unpublished Ph.D. thesis, Indiana University), http://files.dubfire.net/?csoghoian-dissertation-final-8-1-2012.pdf (noting that between 2000 and 2011, encryption was encountered in the course of executing 109 state and federal wiretaps, but that in none of those cases did the encryption prevent officials from obtaining the contents of communications).

32 United States v. Jones, 132 S. Ct. 945, 963–64, 964 n.10 (2012) (Alito, J., concurring in the judgment); *see also* United States v. Knotts, 460 U.S. 276, 277–80 (1983).

33 *Jones*, 132 S. Ct. at 948.

34 Many cars come equipped with the OnStar system, which essentially embeds a cell phone in the car dashboard, or a similar system like those offered by BMW and Mercedes Benz. The OnStar service uses the phone to provide emergency response, hands-free calling, directions, and similar services. Because it is essentially a cell phone, the OnStar system includes both a GPS device and a microphone. Law-enforcement agencies have found both features attractive. *See, e.g.*, United States v. Perez, 440 F.3d 363, 366 (6th Cir. 2006) (DEA agents used OnStar system's GPS capability to track down suspect's Cadillac Escalade); *In re* United States, 349 F.3d 1132 (9th Cir. 2003) (FBI sought order requiring operator of unnamed OnStar-like system to activate system microphone so they could listen to conversations in suspect's car); United States v. Dantzler, No. 10-0024, 2010 U.S. Dist. LEXIS 68753 (W.D. La. June 16, 2010) (magistrate judge's similar report and recommendation); Sherrod v. United States, No. 08-CV-2013, 2008 U.S. Dist. LEXIS 102727, at 6–7 (C.D. Ill. Dec. 19, 2008) (similar); United States v. Coleman, No. 07-20357, 2008 U.S. Dist. LEXIS 12276 (E.D. Mich. Feb. 20, 2008) (similar).

have bypassed cars entirely by tracking suspects' cell phones[35] and license plates.[36] Cell phone tracking in particular has become a routine tool for law enforcement; wireless carriers in the United States receive hundreds of thousands or millions of requests each year for subscriber records, including location information.[37]

Two caveats should be flagged at the outset. First, in referring to costs and benefits, I mean the private costs and benefits to the participants in the information flow, not the social costs and benefits of protecting privacy or privacy generally. Since the participants in an information flow can usually decide whether the information flow will occur or not, and will usually take their own interests into account, these are the costs and benefits that determine behavior.[38] And second, this cost-benefit analysis cannot tell us everything about the likelihood that an information flow will occur; people do not always act rationally, and many actors will have incomplete information about the costs and benefits of an information flow. But there are reasons to think that an incentive analysis can do a decent job, at least in some circumstances. Many of the most important privacy questions today involve the collection, use, and dissemination of information by companies, the government, and other large institutions. Although these institutions do not always act ration-

35 *See, e.g.*, United States v. Skinner, 690 F.3d 772, 781 (6th Cir. 2012) (holding that the defendant had no reasonable expectation of privacy in the location of his cell phone, and thus that police did not violate the Fourth Amendment in tracking its location).

36 *See, e.g.*, Veronica Gonzalez, *Police License Plate Readers Come Under Fire*, VIRGINIAN-PILOT (Hampton Roads, Va.) (Aug. 3, 2012), http://hamptonroads.com/2012/08/police-license-plate-readers-come-under-fire; Christine Vendel, *KC Police Hold a Treasure Trove of License Plate Data*, KAN. CITY STAR (Mo.) (July 30, 2012), http://www.kansascity.com/news/local/article306332/KC-police-hold-a-treasure-trove-of-license-plate-data.html.

37 Soghoian, *supra* note 31, at 24; *see also* Eric Lichtblau, *Police Are Using Phone Tracking as a Routine Tool*, N.Y. TIMES (Mar. 31, 2012), http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html; Declan McCullagh, *Feds Push for Tracking Cell Phones*, CNET (Feb. 11, 2010, 4:00 AM), http://news.cnet.com/8301-13578_3-10451518-38.html. As Soghoian points out, the ability of third-party service providers to automatically record and provide access to subscriber records has been a critical factor reducing the cost of performing surveillance for law enforcement. Soghoian, *supra* note 31, at 32–36. In response to the *Times* story, Representative Edward Markey wrote to nine wireless carriers seeking information about how often they release subscriber information to law-enforcement agencies. Responses revealed how commonly used a tool cell-phone tracking has become. For instance, Sprint reported that in five years, it had received approximately 52,000 court orders for wiretaps, 78,000 court orders for installation of a pen register or trap-and-trace device, 196,000 court orders for location information, and 500,000 subpoenas from law enforcement. Letter from Vonya B. McCann, Senior Vice President, Sprint Nextel, to Rep. Edward J. Markey 4 (May 23, 2012), web.archive.org/web/20130415200646/http://markey.house.gov/sites/markey.house.gov/files/documents/Sprint%20Response%20to%20Rep.%20Markey.pdf. Likewise, Verizon Wireless reported that in 2012, it received 270,000 requests from law-enforcement agencies for customer information, about half of which were subpoenas. Letter from William B. Petersen, Gen. Counsel, Verizon Wireless, to Rep. Edward J. Markey 1–2 (Oct. 3, 2013).

38 This point is developed in Section II.A.

ally, they do seem more likely than many individuals to calculate and respond to their own incentives.

A. Benefits

Information subjects and others obtain many different kinds of benefits from information flows. Although we can broadly classify these benefits as business or personal in character, each category contains numerous benefits of different kinds.

Some benefits relate to the business interests of a participant. These business benefits come in different forms. In some cases, the information collected, used, or disseminated is itself valuable to the participant's business, such as when a private investigator collects information about a target or when a magazine publisher disseminates information about a celebrity or politician. In other cases, information flows allow businesses to understand their markets and adjust business practices accordingly. Apple, for instance, uses its Genius Bars to learn more about what goes wrong with its products as customers use them, so it can gradually improve its products.[39] Similarly, Best Buy analyzed data about customer transactions to develop profiles of different types of customers and to train its employees to concentrate on the most profitable ones.[40] In other cases, more information allows businesses to make better predictions about future events, as when financial institutions use credit reports to predict customer risk or when stores use customer-survey data to predict future demand. It is impossible to classify all the ways participants obtain business benefits from information flows, which will be as varied as the many different kinds of businesses that engage in information flows, but these examples show a few of the possibilities.[41]

Other benefits of information flows are personal in nature, and just as business benefits correspond to a wide variety of business practices, personal benefits from information flows can correspond to innumerable parts of people's lives. Information flows are essential for people to form associations with one another. For instance, people will necessarily learn about each other in the course of forming and maintaining a friendship, business partnership, or romantic relationship, and those information flows will help maintain and develop the relationship over time. Information flows are also

39 *E.g.*, James Duncan Davidson, *A Hidden Genius at the Apple Store*, JD² WEBLOG (Oct. 26, 2010), http://web.archive.org/web/20121221084345/http://duncandavidson.com/blog/2010/10/apple-store. The web travel site Kayak.com takes a similar approach to improving its website: customer-service calls are answered by company engineers instead of dedicated support personnel, so they have an immediate incentive to make the site better and reduce the number of support calls. *See* Liz Welch, *The Way I Work: Paul English of Kayak*, INC. (Feb. 1 2010), http://www.inc.com/magazine/20100201/the-way-i-work-paul-english-of-kayak.html.

40 *See* Gary McWilliams, *Analyzing Customers, Best Buy Decides Not All Are Welcome*, WALL ST. J. (Nov. 8, 2004, 11:59 PM), http://www.wsj.com/articles/SB109986994931767086.

41 *Cf.* Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 394–97 (1978) (reviewing the "demand for private information").

essential for learning about the world; a student cannot learn history, for instance, without absorbing information about others that has been collected and disseminated by various outsiders. And people gain intangible psychological benefits from information flows, such as the emotional satisfaction from fulfilling a simple curiosity. As before, this is far from a comprehensive account of personal benefits from information flows, but it shows the broad scope and diverse nature of such benefits.[42]

Many of the business and personal benefits from information flows are symmetrical, or at least similar, between information subjects and outsiders, but others are notably different. Two people forming a friendship, business partnership, or romantic relationship, for example, will benefit mutually from exchanging information as they build the trust, intimacy, and a common base of knowledge that will inform their relationship going forward. Likewise, a credit-seeking consumer who provides information to a bank reduces the information asymmetry between herself and the bank, allowing the bank to better assess her risk and potentially leading to a credit transaction desired by both sides. But sometimes different participants will obtain different kinds of benefits from an information flow. A psychiatrist asking about a patient's life to help diagnose or treat psychiatric problems, for instance, benefits from information that helps her provide professional services, while the patient obtains decidedly personal benefits from the same information flow. A reader of a gossip magazine obtains entertainment value from reading about a celebrity romance, while the magazine gains advertising and sales revenue, and the celebrities add to their fame and future bankability. And sometimes, only some participants will benefit from the information flow, such as when police surveil a suspect, when a bank uses a credit report to reject a credit applicant, or when a magazine publishes information the subject would prefer not be published. In each of these information flows, another participant or participants may not know about the information flow, or may actually be harmed by it.

B. Costs

The costs of information flows are more easily classified than the benefits. At the broadest level, participants face both direct costs of implementing the information flow itself and consequential costs that arise due to the information flow. A police department following a suspect, for instance, will incur direct costs carrying out the surveillance: the value of the officers' time; the opportunity cost from foregoing other investigations; maybe incidental expenses like the cost of gas (if traveling by car) or transit fare (if traveling by

42 There are also benefits that flow (no pun intended) to non-participants in the information flow. For instance, some information flows provide broad public benefits, like the public-safety benefits from police and prosecutors using information to prevent, investigate, and prosecute crimes. These benefits are less relevant to our cost-benefit analysis, since they have only a secondary effect, if any, on a decisionmaker's calculation of whether to cause the information flow to occur.

bus or train). The suspect, presumably unaware of the surveillance, faces no such direct costs, since any expenses are just those she would have incurred anyway, but may incur costs as a result of the surveillance, such as an increased likelihood of criminal prosecution and conviction.

These costs can also be classified by their source, as costs from technology, costs from social norms or society, and costs from law. Any of these things can make a given information flow more or less costly for different participants:

1. Costs from Technology

Technology is often recognized as raising privacy problems by making certain types of information flows easier. Yet technology can make information flows either more or less costly for the participants.

We've already seen a few examples of technology making information flows less costly, as in the shopping mall and GPS examples: technology made it far easier to track shoppers and suspects by replacing time-consuming personal observation or error-prone surveys with automatic electronic tracking. Other examples are legion[43]: security cameras reduce the cost of monitoring an area; the federal courts' PACER system (Public Access to Court Electronic Records) reduces the cost of obtaining information stored in court records;[44] data analytics software reduces the cost of drawing inferences from consumer behavior. Nor is this a new phenomenon; as long ago as 1890, Warren and Brandeis complained that "the latest advances in photographic art have rendered it possible to take pictures surreptitiously," rather than requiring a subject to pose for an extended time.[45]

While somewhat less common, technology can also make information flows more costly for participants. For instance, technology can make defensive self-help easier, or even possible, helping information subjects protect themselves from unwanted information flows. Encryption technologies are the classic example, but tinted windows, noise machines, disguises, radio-frequency jammers, steganography, throw-away email addresses, radar detectors, and cookie blockers are all technologies that raise the cost of collecting, using, and disseminating information about someone.[46] Technology can

43 Helen Nissenbaum devotes three chapters of *Privacy in Context* to the myriad ways information technologies have threatened privacy, usually by reducing the cost of information flows, though she does not put it in those terms. NISSENBAUM, *supra* note 17, at 19–64.

44 *See generally* Amanda Conley et al., *Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry*, 71 MD. L. REV. 772, 816 (2012).

45 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 211 (1890).

46 The TrackMeNot web-browser plugin is another good example. TrackMeNot is designed to make it harder for search engines and ad networks to make accurate inferences about a user. TrackMeNot works in the background, making hundreds of irrelevant requests to search engines like Google and Bing. Since a user's genuine searches cannot easily be separated from the sea of irrelevant searches, search engines and advertisers that use search information cannot draw useful conclusions about a user's interests and prefer-

also cause more information to be created and stored, raising the cost of reviewing and analyzing information. The rise of computers has made investigating financial crimes more costly than before, for instance, because investigators may have to painstakingly review hundreds of thousands or millions of files, and countless emails, to piece together relevant evidence. And advances in one technology can make other technologies less effective at facilitating information flows. For instance, the switch from circuit-switched telephone networks to packet-switched networks and the substitution of cell phones for landlines made it harder to wiretap phone calls. Likewise, some technology companies have taken steps to make it harder to access information that is stored in or travels through their products, to the deep annoyance of law-enforcement officials.[47]

2. Costs from Social Norms or Society

Other costs of information flows stem from social consequences of information flows, determined by norms and other social structures. As with changes in technology, evolving norms can increase or reduce these costs.

For an information subject, these costs largely take the form of reputational harm and other negative inferences people draw from information.[48] If a journalist, or an errant Google search, reveals something embarrassing about someone—say, that the subject was arrested for drug possession, had an affair, or embezzled from a former employer—that information could obviously harm the subject. He or she might have a hard time finding a job or maintaining a marriage; friends or business contacts may drift away. The magnitude of this harm depends on the norms about the particular piece of information revealed, which often vary greatly over time, in both directions.

---

ences. *See* Daniel C. Howe & Helen Nissenbaum, *TrackMeNot: Resisting Surveillance in Web Search*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 417, 420–25 (Ian Kerr et al. eds., 2009); TRACKMENOT, http://cs.nyu.edu/trackmenot/ (last visited Jan. 27, 2016).

47 *See, e.g.*, Andrea Peterson & Ellen Nakashima, *Obama Administration Explored Ways to Bypass Smartphone Encryption*, WASH. POST (Sept. 24, 2015), https://www.washingtonpost.com/world/national-security/obama-administration-ponders-how-to-seek-access-to-encrypted-data/2015/09/23/107a811c-5b22-11e5-b38e-06883aacba64_story.html; Craig Timberg, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html; Craig Timberg & Greg Miller, *FBI Blasts Apple, Google for Locking Police Out of Phones*, WASH. POST (Sept. 25, 2014), http://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html; Cyrus R. Vance Jr. et al., Opinion, *When Phone Encryption Blocks Justice*, N.Y. TIMES (Aug. 11, 2015), http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html.

48 On reputational harm, see ROBERT C. ELLICKSON, ORDER WITHOUT LAW 52–58, 232–33 (1991), DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (2007), LIOR JACOB STRAHILEVITZ, INFORMATION AND EXCLUSION 127–33 (2011), and Lior Jacob Strahilevitz, *Reputation Nation: Law in an Era of Ubiquitous Personal Information*, 102 NW. U. L. REV. 1667, 1670–1710 (2008).

An admission of past marijuana use, for instance, sunk Douglas Ginsburg's nomination to the Supreme Court in 1987.[49] Later admissions of drug use, however, had far smaller effects, creating minor controversies for Clarence Thomas,[50] Bill Clinton,[51] and Barack Obama.[52] Similarly, information that someone is gay is less damaging today than it was ten, twenty, or fifty years ago. Information about someone's racist beliefs, in contrast, would likely be more damaging today than it would have been decades ago.[53] And these social dynamics extend far beyond core beliefs like attitudes about civil rights; changes in norms and reputation extend to areas as specific as attitudes about how far kids should roam from home unsupervised, a surprisingly controversial subject.[54]

The social costs to outsider participants of information flows are likewise reputational, but they arise in a different way. Information flows tell us something about outsiders not because we can draw inferences from the content of the information, but because we can draw inferences from the existence of the information flow in the first place. The fact that someone cares enough about someone else to collect, use, or disseminate information about that person may be benign, but it can also seem curious, odd, or creepy. No one blinks an eye when a dating website asks someone about his or her romantic preferences, collecting information about a user, but it would be strange if Amazon, or the DMV, started asking shoppers or applicants for driver's licenses if they prefer blondes or brunettes. Seeking such information would likely impose a social cost on Amazon and the DMV: some fraction of shoppers would see Amazon as creepy and take their shopping elsewhere, while some applicants would complain, put political pressure on DMV management, or file lawsuits. As Helen Nissenbaum has explained, these norms of information flows will vary greatly from context to context, based on the fea-

49 Susan M. Olson, *Ginsburg, Douglas Howard*, *in* THE OXFORD COMPANION TO THE SUPREME COURT OF THE UNITED STATES 392 (Kermit L. Hall et al. eds., 2d. ed. 2005).

50 *E.g.*, Stephen Labaton, *Thomas Smoked Marijuana but Retains Bush Support*, N.Y. TIMES (July 11, 1991), http://www.nytimes.com/1991/07/11/us/thomas-smoked-marijuana-but-retains-bush-support.html.

51 *E.g.*, *Clinton Tried Marijuana as a Student, He Says*, N.Y. TIMES (Mar. 30, 1992), http://www.nytimes.com/1992/03/30/news/30iht-bill_1.html.

52 *E.g.*, Katharine Q. Seelye, *Barack Obama, Asked About Drug History, Admits He Inhaled*, N.Y. TIMES (Oct. 24, 2006), http://www.nytimes.com/2006/10/24/world/americas/24iht-dems.3272493.html; *see also* BARACK OBAMA, DREAMS FROM MY FATHER 93 (Crown 2004) (1995).

53 As recently as 1968, George Wallace won five states and forty-six electoral votes, running for president on an openly segregationist platform—a result that would be unimaginable today.

54 For instance, parents have been arrested for letting kids walk to nearby destinations unsupervised. *See, e.g.*, Lenore Skenazy, *Outrage of the Week: Mom Arrested for Letting Her Kids, 11 & 7, Walk to Pizza Shop*, FREE-RANGE KIDS (July 17, 2012), http://www.freerangekids.com/outrage-of-the-week-mom-arrested-for-letting-her-kids-11-7-walk-to-pizza-shop-2/; *see also* LENORE SKENAZY, FREE-RANGE KIDS (2009).

tures of a context, the actors involved in the context, the attributes of the information, and various transmission principles.[55]

As with reputational costs to information subjects, these reputational costs to outsiders are not static, but change over time. Many of these norms have become more permissive as information flows become more common. More and more companies collect personal information and use it to target advertising, for instance, while consumers arguably care less and less. Google's Gmail service, for instance, was somewhat controversial at its launch, since it scans the contents of messages to serve ads based on the contents of email messages, but in the years since, complaints have largely died down.[56] Likewise, location tracking of the kind that Path Intelligence markets to shopping mall operators has become less controversial.[57] But other norms have become less permissive, or more protective of privacy, so that the social cost of engaging in an information flow increases. Voting, for instance, was typically conducted out in the open until the secret ballot became standard in the 1880s and 1890s.[58] Grades and other educational records were often publicly posted, or otherwise not considered especially sensitive, before the Family Educational Rights and Privacy Act of 1974.[59] And before 2007, filings in federal court often contained sensitive information, such as Social Security numbers, the names of minors, dates of birth, and financial account numbers; now, such information is routinely

55 *See, e.g.*, NISSENBAUM, *supra* note 17, at 129–57.

56 *See, e.g.*, *Gmail Privacy FAQ*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/gmail/faq.html (last visited Jan. 27, 2016) (arguing that "Gmail violates the privacy rights of non-subscribers" because their emails may be monitored and saved without consent); Saul Hansell, *The Internet Ad You Are About to See Has Already Read Your E-Mail*, N.Y. TIMES. (June 21, 2004), http://www.nytimes.com/2004/06/21/business/media-business-advertising-internet-ad-you-are-about-see-has-already-read-your-e.html; Mark Rasch, *Google's Gmail: Spook Heaven?*, REGISTER (June 15, 2004, 9:46 AM), http://www.theregister.co.uk/2004/06/15/gmail_spook_heaven/ (arguing that Gmail "represents a disturbing conceptual paradigm—the idea that computer analysis of communications is not a search").

57 *See supra* text accompanying note 8. Though there are signs that people still distrust location tracking, at least when put in the government's hands. For instance, in late 2012, the Transportation Security Administration tested a system that estimated wait times at airport security checkpoints by using Bluetooth to detect how long individual cell phones were located near the checkpoint. The agency abandoned the program after testing it in two airports. *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR AUTOMATED WAIT TIME (AWT) TECHNOLOGY (2012), http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_tsa_awt_august2012.pdf; Scott MacFarlane, *Records Show TSA Tracked Bluetooths to Observe Wait Times*, WSBTV.COM (Mar. 20, 2013, 5:04 PM), http://www.wsbtv.com/news/news/local/documents-show-tsa-tracked-bluetooth-devices-monit/nWyb3/.

58 *See, e.g.*, Pamela S. Karlan, *Elections and Change Under* Voting with Dollars, 91 CALIF. L. REV. 705, 708–10 (2003).

59 Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2012).

redacted.[60] Each of these examples involves law requiring the change, but such laws are typically a reaction to changing norms.[61]

3. Costs from Law

Finally, law itself can change the cost of an information flow, both for information subjects and for the other participants in the information flow. The law has several mechanisms to do this. Most directly, it can reward or punish information flows—so-called carrot and stick strategies—by imposing costs or benefits (i.e., negative costs) on the parties engaging in an information flow. Numerous privacy laws work this way. Laws forbidding information disclosures, for example, impose costs on parties that nevertheless disclose information.[62] Laws permitting the collection and use of information, but imposing restrictions or regulations, often impose significant compliance costs. Laws encouraging cooperation between private entities and government agencies, on the other hand, reward information flows, at least when they benefit the government.[63]

The law can also use what Lior Strahilevitz has called curtain and searchlight strategies. Curtain strategies make information obscure so that it is harder for private actors to use the information.[64] Rather than imposing direct costs like compliance costs on private actors, they make it harder to obtain or use information. Searchlight strategies do the opposite: they shine light on information, making it more accessible and easier to obtain and

60 *See* FED. R. CIV. P. 5.2 (requiring parties to redact such sensitive information in filings in federal district courts).

61 The secret ballot might be an exception to this rule, with secrecy rules possibly enacted to help entrench the power of the existing political parties. *See* Karlan, *supra* note 58, at 708–10.

62 Educational institutions that violate the Family Educational Rights and Privacy Act, for instance, can lose federal funding. *See* 34 C.F.R. § 99.67 (2014). The Department of Health and Human Services has taken numerous enforcement actions against medical providers that violated privacy provisions of the Health Insurance Portability and Accountability Act. *See, e.g.*, *Health Information Privacy: Case Examples and Resolution Agreements*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html (linking to press releases covering numerous HIPAA settlements) (last visited Jan. 27, 2016).

63 Federal law, for instance, immunizes telecommunications providers from liability for sharing information with the federal government for certain intelligence purposes. FISA Amendments Act of 2008 § 802, 50 U.S.C. § 1885a (2012). Likewise, interception orders issued pursuant to the Electronic Communications Privacy Act give telecommunications service providers an incentive to share information with law-enforcement agencies by removing a potential cost for those that do, and imposing costs on those that refuse. *See* 18 U.S.C. § 2518(4) (2012) ("Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance."); *id.* § 2518(12) (providing that service providers may move to quash an interception order, but leaving the cost of so moving to service providers).

64 STRAHILEVITZ, INFORMATION AND EXCLUSION, *supra* note 48, at 157–58.

use.[65] Much information disclosure by the government falls into this category, from the publication of securities filings and criminal records to the mandated placement of hygiene ratings at the entrances to restaurants in New York, Los Angeles, and Beijing.[66] Likewise, many laws mandate disclosure, in an effort to counter irrational behavior or cure information asymmetries, making it easier for recipients to use that information in making their own decisions.[67] And when information is disclosed, laws can make that information easier or harder to use, for instance by requiring electronic filing or making the information available in a standardized form with API access.[68]

* * *

All of these costs and benefits can come into play when information flows occur. Predicting what information flows will occur, though, requires more than just adding up costs and benefits; the structure of information flows means that some costs and benefits matter more than others. The next Part discusses how to use the costs and benefits of information flows to predict which information flows will occur.

II. A Probabilistic Account of Privacy

Privacy is a field dominated by normative arguments, debating what information is sensitive, personal, or intimate enough to be considered private, or what information should receive legal protection. Privacy scholars have developed fewer tools for describing how widely known a particular piece of information is. Yet this descriptive sense of privacy is as important, for two reasons. First, a descriptive account of how public or private information is matters in several areas of the law, from the Fourth Amendment to tort law to intellectual property and trade secrecy. In each of those areas of law, the fact that information becomes more available or more known to more of the public can have legal consequences, regardless of whether the information is in some way sensitive, personal, or intimate. And second, evidence shows that individuals care greatly about this descriptive form of privacy and the degree to which information about them is available to or

65 *Id.* at 158–59.

66 *Id.*; Evelyn Iritani, *Not Much Faith in Their Food*, L.A. Times (Jan. 23, 2007), http://articles.latimes.com/2007/jan/23/world/fg-chifood23.

67 *See generally* Omri Ben-Shahar & Carl E. Schneider, More than You Wanted to Know (2014).

68 As one example, Senate campaign-finance reports are filed on paper, while House reports are filed electronically, making it much easier to review the House reports. Kathy Kiely, *Voting in the Dark: Senate Hides $57 Million in Campaign Contributions Behind Thicket of Dead Trees*, Sunlight Found. Blog (Oct. 28, 2014, 10:49 AM), https://sunlightfoundation.com/blog/2014/10/28/voting-in-the-dark-senate-hides-57-m-in-campaign-contributions-behind-a-thicket-of-dead-trees/. Groups like the Sunlight Foundation help make this information more readily available, but they cannot completely close the gap.

known by others, even when the information is not sensitive, personal, or intimate.

The costs and benefits described in Part I can help provide such a descriptive account of privacy. This Part develops that account. First, I argue that in many cases, an outsider, rather than the information subject, decides whether the information flow will occur. Because such a potential unilateral invader acts according to his or her own incentives, it is his or her own private costs and benefits that matter. Second, I discuss two models of unilateral invaders' decisionmaking about whether an individual information flow will occur: a traditional rational-choice model and a stochastic-choice model that better accounts for real-world behavior in the face of uncertainty. Finally, I shift to the perspective of an information subject, discussing how aggregating individual information flows can provide a model for the privacy an individual enjoys in any given type of information.

A. Unilateral Invasions

Not all costs and benefits are equal, and simply listing and comparing the costs and benefits to the participants in an information flow does not always tell whether the information flow will happen. Often, the benefits will outweigh the costs for one participant in an information flow, while the costs will outweigh the benefits for another participant. Ideally, we might want such an information flow to occur if the total benefits will exceed the total costs, but the mechanics of the participants' decisionmaking does not always lead to that outcome.

Instead, in many information flows, a single participant who is not the information subject makes a unilateral decision that the information flow will occur. This person, the relevant decisionmaker, acts (at least, within this simplified model) according to his or her own incentives, so that the information flow occurs if and only if the benefits to the decisionmaker outweigh the costs to the decisionmaker, regardless of the effect on total welfare. This decisionmaker is the participant whose behavior is sensitive to changes in incentives, such that if his or her costs or benefits of engaging in the information flow change, the likelihood that the information flow will occur also changes. And, critically, I claim that for many information flows—including the information flows at issue in the most important privacy problems—the principal determinant of whether the information flow occurs is an outsider rather than the information subject.

This unilateral decisionmaking can take different forms. The clearest example comes when the information subject is unaware of the information flow. For example, if a private investigator or detective is doing his or her job right, the target of surveillance will have no idea he or she is being followed; the investigator determines unilaterally, without the target's input, whether to collect information (perhaps with the input of other outsiders, such as a client or supervisor). Likewise, many people are unaware of the many common forms of commercial tracking, such as cookie tracking by online ad networks, tracking databases used by marketers and political campaigns to target

potential customers and voters, and tracking of phones' physical locations by wireless carriers.[69] In these cases, only one participant in the information flow—the investigator, ad network, or database operator—is even aware of its existence. Since that participant gets to make a unilateral decision whether the information flow will occur, and can give full weight to his or her own incentives, the information flow will occur if and only if it is in his or her interests.

Alternatively, an information subject may be aware of an information flow, but unable to do anything about it. One common example arises when information about someone is published or otherwise disseminated without the subject's consent. A celebrity featured in a tabloid exposé, for example, likely knows that information about him- or herself is being disseminated to the public, as might a subject of gossip in a close-knit community, but likely neither can stop the information flow. Likewise, attorneys handling defamation cases or seeking to have information removed from the Internet have to consider the Streisand effect, in which information that someone tries to conceal becomes much more widely disseminated.[70] Information can also be collected and used with a subject's knowledge, but without his or her consent, such as when a credit bureau compiles information about a consumer and infers his or her creditworthiness. (This scenario also applies when an information subject is compelled to provide information, by law or otherwise.)

Information subjects can also be aware of a general category of information collection, use, or dissemination, without being aware of the specifics of any particular information flow. Many Internet users know, for instance, that companies track their behavior online and use it to target ads, but most users would be surprised by the number of tracking companies and the sheer scope of such tracking.[71] And although many consumers know that retailers track individuals' purchases, often through loyalty cards that provide discounts, they may be surprised to learn that such tracking occurs even without loyalty cards. Target, for instance, has no general loyalty card, but it nevertheless tracks purchases using debit and credit card numbers and personalized coupons, along with information purchased from commercial databases. Using such techniques, it has become quite good at predicting customers' future purchasing behavior.[72] Yet as one Target statistician told the *New York*

69 *See, e.g.*, Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 273 (2012).

70 The effect is named for Barbara Streisand, who sued to have a photograph of her beachfront house removed from a public database of 12,000 coastline photos. Before the lawsuit, the photo of Streisand's house had been downloaded six times, including twice by Steisand's attorneys. After Streisand filed the lawsuit, the photo was seen by hundreds of thousands of people. *See, e.g.*, Jonathan Zittrain, *The Fourth Quadrant*, 78 FORDHAM L. REV. 2767, 2774 & n.10 (2010).

71 *See, e.g.*, Hoofnagle et al., *supra* note 69, at 273.

72 *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html; Kashmir Hill, *How Target Figured out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16,

Times Magazine, these predictions must be used carefully, or customers get creeped out:

> "If we send someone a catalog and say, 'Congratulations on your first child!' and they've never told us they're pregnant, that's going to make some people uncomfortable," Pole told me. "We are very conservative about compliance with all privacy laws. But even if you're following the law, you can do things where people get queasy."[73]

Likewise, even if a consumer might know about one aspect of an information flow, she often cannot or will not know everything the outsider does with information. An informed consumer who knows that a website tracks her activities may not know, for instance, everything the website does with the information, or to whom it sells that information.[74]

Indeed, in some circumstances, observers rely on information subjects having general, but not specific, knowledge of tracking. Automated speeding and red-light cameras are intended (in part) to discourage unsafe traffic behavior, so drivers must know there is a chance they will be observed speeding or running a red light. Sometimes police make these cameras obvious, so they will have an effect in a particularly sensitive or dangerous spot. But sometimes they simply announce that cameras will be installed, or will be in force on specific dates, to induce a general effect. If drivers knew precisely where cameras were stationed, they could confine their safer driving to those areas; only if drivers lack that knowledge can the cameras have their full desired effect.

In some of these circumstances, it is debatable whether the information subject or the outsider is the true decisionmaker. Many consumers, for instance, know that credit bureaus compile information about financial transactions and use it to prepare and sell credit reports. Arguably, they could prevent these information flows by opting out of entire categories of financial transactions. Yet because the costs of opting out would be so great compared to the benefits of doing so, arguably consumers are compelled to submit to the credit-reporting system. Regardless, on the margin the relevant decisionmaker seems likely to be the outsider: a financial company or credit bureau can increase the amount of tracking it does—by adding new variables, collecting data from new sources, or integrating additional databases

---

2012, 11:02 AM), http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

73 Duhigg, *supra* note 72.

74 This problem is compounded by the common practice of companies writing privacy policies that reserve broad and vague rights to use data. *See, e.g.*, FED. TRADE COMM'N, WHAT'S THE DEAL? AN FTC STUDY ON MOBILE SHOPPING APPS 1 (2014), http://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf ("[A]lthough nearly all of the apps made strong security promises and linked to privacy policies, most privacy policies used vague language that reserved broad rights to collect, use, and share consumer data, making it difficult for readers to understand how the apps actually used consumer data or to compare the apps' data practices.").

into its data set—without significantly changing marginal consumer behavior.

The essential role outsiders play in all of these kinds of information flows follows from the basic nature of these information flows. Collecting, using, and disseminating information are all activities that can both be conducted by, and inure to the benefit of, outsiders, with or without affecting the information subject. Collecting information about a person, for instance, is something that outsiders can often do unilaterally; an information subject, on the other hand, would rarely need to collect information about him or herself, since he or she likely possesses near-complete information. Information use, likewise, frequently requires processing or aggregating information from readily available public sources, or using certain information to infer other facts about people, none of which an information subject is likely to need to do. And anyone can disseminate information once he or she possesses it, regardless of the subject's knowledge or consent; the trick is to acquire the knowledge in the first instance.

To distinguish outsider-initiated information flows from those initiated by the information subject, I call those in the former "invasions." Invasions are characterized by the outsider's intent to collect, use, or disseminate information about a subject.[75] That does not mean all such invasions are unwelcome or unwanted by the information subject; many types of information collection, use, and dissemination benefit, or at least do not harm, information subjects. For instance, credit reporting presumably benefits consumers with good credit histories; such a consumer will probably welcome the credit bureau's information collection and use.[76] But because credit bureaus and other outsiders that initiate invasions make unilateral decisions to collect, use, and disseminate information, that information becomes more broadly available to people other than the information subjects. Due to no action of his or her own, information about the information subject is less private—is more available to others—than it otherwise would have been.

Certainly not every information flow is a unilateral invasion; information subjects do decide to make information about themselves available for others to collect, use, and disseminate. But unilateral invasions are of critical importance in privacy law and theory, for two reasons. First, unilateral invasions are far more likely than other information flows to create privacy problems. Even if a significant number of information flows are initiated by information subjects, such cases are likely to be less significant for privacy law than those initiated by outsiders, because information subjects presumably consent to information flows they themselves initiate; otherwise they would not have

75 Dictionary definitions of "invade" include "[t]o infringe, or encroach on," *Invade*, WEBSTER'S NEW INTERNATIONAL DICTIONARY 1304 (2d ed. 1941), and "encroach or intrude on: '*he felt his privacy was being invaded*'." *Invade*, OXFORD ENGLISH DICTIONARY (2d ed. 1989), http://www.oxforddictionaries.com/us/definition/american_english/invade (last visited Jan. 29, 2016).

76 This may be especially true for individuals who might otherwise suffer from discrimination. *See* STRAHILEVITZ, *supra* note 48, at 81.

made the decision that the information flow proceed. And second, unilateral invasions help shed light on some of the most interesting and important dilemmas in modern privacy law. Behavioral advertising, location tracking, data mining, and other modern commercial tools depend on unilateral invasions, since outside trackers must be able to unilaterally collect, use, and disseminate data about others. Likewise, many of the most controversial modern law-enforcement and national-security measures depend on the unilateral collection, use, and dissemination of information about individuals, including the GPS tracking at issue in *Jones,* the thermal imaging at issue in *Kyllo v. United States,*[77] the NSA's warrantless wiretapping program, and use of drone aircraft in both domestic law enforcement and overseas military operations.

B. Rational-Choice and Stochastic-Choice Models of Information Flows

An outsider who decides whether a given information flow will occur is more likely to engage in that information flow when its benefits outweigh its costs. And though this statement may seem obvious, it provides a surprisingly useful tool for considering privacy in a changing society. This subsection discusses two models of the decision to engage in an individual information flow based on this idea.

The most basic model of a decision to engage in an information flow is a rational-choice model, which proposes that the decisionmaker will engage in the information flow if and only if its private benefits exceed its private costs. Consider a relatively simple example: the use of license plates by police officers. License plates can provide various kinds of information about a driver. The plates alone can provide some basic information, such as whether the driver is local or from out of state, or, when the plates are personalized, a sense of the driver's personality. More information, such as the driver's name and age, can be obtained by looking up the license-plate number in a database. And the sheer act of spotting the license plate at a particular place and time can reveal that the driver was nearby at that time. Collecting and using license-plate information, though, has usually been relatively costly for law enforcement: it took time to observe and do something with a car's license-plate number, like looking up information about the car or driver in a database. So license plates have historically been used as a law-enforcement tool when needed in two kinds of cases: when a license-plate number has been linked to a particular crime or suspect, and when a police officer observes a traffic violation.

In each of these cases, the cost-benefit analysis could come out in favor of the information flow. When a license-plate number has been linked to a particular crime, the number of information flows required to track down the suspect might be large, but the cost of each information flow is very small. For instance, if a witness sees the license plate on a bank robber's getaway car, police can be on the lookout for that license plate at little cost

77 533 U.S. 27 (2001).

for each observation. Say the cost is $1 for each time an officer looks at a car to see if it matches the description of the suspect's car, in officer time, opportunity costs from not pursuing other crimes, and so forth. If the benefit of capturing a specific suspect is high—say, $50,000 for a bank robber—then the information flow is worthwhile even if each observation has only a 0.01% chance of finding the right car.[78] A police department is thus likely to devote its resources to those information flows.[79]

When an officer sees a specific traffic violation and can stop the driver without searching for a specific license plate, the cost of the individual information flow is somewhat higher, since it takes more time to pull over a driver, check a database for notes about the car and driver, and process a traffic stop than to glance at a license plate. Say this cost is $20 in officer time and database costs. But because the cost is incurred only once, with no speculation or trial and error, it can be outweighed by even a relatively small benefit. If the benefit of stopping a driver who ran a red light is $100 (in the likely fine paid by the driver and in safety and deterrent effects from enforcing traffic laws), the benefit outweighs the $20 cost, and the information flow is cost-efficient. But if the cost were less certain—if, for instance, a witness wrote down the license-plate number for a car that ran a red light and officers needed to check different plates to find the right car—then the information flows would not be cost effective.[80] The bottom line, then, is that a particular category of information flows—reviewing license plates to catch criminals—would occur only in the limited circumstances when it was especially valuable.

This account of the cost-benefit analysis of using license plates made sense when license-plate numbers could only be read by humans. In the last decade, however, automatic license-plate recognition technology has turned this analysis on its head and greatly expanded the universe of cost-efficient information flows.[81] Recognition devices take photographs of cars' license plates and use optical character recognition to determine and record the license-plate number. Because they can operate automatically, either from a stationary position or while attached to a police car, they reduce or eliminate the marginal cost of looking for specific license-plate numbers. So while nothing changes in the example of an officer witnessing a traffic violation, things are different when a plate number of interest has been identified. Instead of $1 per observation, the cost of checking a plate number to see if it matches might be 1¢ or even 0.01¢. Before it only made sense to check license-plate numbers when a specific car was being sought in connection

78 The expected value of each observation is $50,000 × 0.01% = $5, well above the $1 cost.

79 This assumes a police department is the relevant decisionmaker, since the department sets its officers' agendas, but the same point applies if you assume officers are independent actors, obtaining benefits in the form of recognition, prestige, or promotion.

80 If we assume the same 0.01% chance of spotting the right license plate, then the expected value of each observation is $100 × 0.01% = 1¢, well below the $1 cost.

81 *See, e.g.*, Gonzalez, *supra* note 36.

with a major crime, as when a getaway car has been identified or a kidnapper is on the run.[82] Suddenly, it might be cost-efficient to search for a car even when the crime is as minor as a traffic violation,[83] or to automatically check every license plate against a list of cars involved in crimes.[84] License plates became, in effect, *less private* without becoming more sensitive or personal: people were more likely to observe and use license-plate information when it became less costly to do so.

Besides making these two scenarios more affordable, recognition devices make other uses of license plates possible for the first time. For instance, several European cities use recognition technology to enforce congestion taxes, which charge vehicles in busy city centers during peak hours.[85] Such a system can operate more cheaply, with better enforcement, than alternatives like tolling or paid permits. And both federal and local law-enforcement officials have begun to make purely speculative use of recognition technology, observing plate numbers and recording their locations in databases.[86] Such a database can show that a particular car was seen in a particular place at a particular time, information that might later prove valuable in a criminal investigation. If the same car happened to be spotted near each of a string of similar muggings, for instance, it might indicate that someone connected with that car was involved in the crimes. Because the marginal cost of each

82 For instance, the AMBER Alert system publicizes information about in-progress kidnapping cases, in the hopes that members of the community will spot and report information about these cases. AMBER Alerts often include information about the suspect's car, including its license-plate number. *See, e.g.*, Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281, 285; Sabrina A. Lochner, Note, *Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans*, 55 ARIZ. L. REV. 201, 225 (2013).

83 Under our previous assumptions, that a scan has a 0.01% probability of spotting the right license plate, and that the value of spotting the right plate in the case of a traffic violation is $100, the expected value of each scan is $100 × 0.01% = 1¢, the same as the cost of each scan.

84 *Cf.* People v. Arden, No. B226290, 2011 Cal. App. Unpub. LEXIS 2737 (Cal. Ct. App. Apr. 14, 2011) (affirming conviction, without significant analysis, for occupying a stolen vehicle when the vehicle was identified as stolen by an automatic license-plate reader).

85 London, Stockholm, and Gothenburg all have these sorts of congestion-pricing systems. Former New York Mayor Michael Bloomberg proposed a similar system for Manhattan, but was unsuccessful in implementing it. *See* Nicholas Confessore, *$8 Traffic Fee for Manhattan Gets Nowhere*, N.Y. TIMES (Apr. 8, 2008), http://www.nytimes.com/2008/04/08/nyregion/08congest.html.

86 *See, e.g.*, Devlin Barrett, *U.S. Spies on Millions of Drivers*, WALL ST. J. (Jan. 26, 2015), http://www.wsj.com/articles/u-s-spies-on-millions-of-cars-1422314779; Gonzalez, *supra* note 36; Christine Vendel, *KC Police Hold a Treasure Trove of License Plate Data*, KANSAS CITY STAR (Mo.) (June 30, 2012), http://www.kansascity.com/news/local/article306332/KC-police-hold-a-treasure-trove-of-license-plate-data.html. The American Civil Liberties Union has launched a project to file public-records requests with local police agencies and determine how different agencies have used license-plate tracking. *See Automatic License Plate Readers*, ACLU, https://www.aclu.org/issues/privacy-technology/location-tracking/automatic-license-plate-readers (last visited Jan. 29, 2016).

automated scan is so low, it can be worthwhile to record and save information even on the bare possibility that it will eventually prove useful.[87]

This rational-choice analysis helps explain decisionmaking in a narrow set of cases, since a rational, risk-neutral decisionmaker with perfect information will engage in the information flow if and only if the private benefit outweighs the private cost. Such a model, though, has its limits: it cannot account for risk-averse decisionmakers, uncertainty in the probability of a favorable outcome, or bounded rationality in decisionmakers. Nor does it provide an account of aggregate behavior across a category of information flows.

To overcome these limitations, economists have developed various stochastic-choice models of decisionmaking given imperfect information.[88] These models assume that decisionmakers do not make a deterministic binary choice to act or not, depending solely on whether the benefits of an action exceed its costs. Rather, they posit that in addition to the action's costs and benefits, a decision is based on other factors that introduce a degree of randomness to the choice.[89] The result is a model that depends on the decisionmaker's cost-benefit analysis, but also accounts for differences due to uncertainty, bounded rationality, and considerations that do not show up in an information flow's costs or benefits. So when the benefits and costs are identical, the information flow will occur with probability 50%.[90] When the benefits are slightly greater than the costs, then the probability of the information flow is greater than 50%, but not by much, and the opposite is true when the costs slightly outweigh the benefits. As the benefits increase

87 One maker of recognition systems brags that its products can capture and process up to 8,000 license-plate numbers per hour, at essentially zero marginal cost. *See T3 Automatic License Plate Recognition System (ALPR)*, T3 MOTION, http://t3motion.com/lpr_page.html (last visited Jan. 29, 2016).

88 *See, e.g.*, CHARLES F. HOFACKER, MATHEMATICAL MARKETING, ch. 15 (2007), http://www.openaccesstexts.org/pdf/Quant_Chapter_15_stochastic.pdf; Thierry Magnac, *Logit Models of Individual Choice*, *in* THE NEW PALGRAVE DICTIONARY OF ECONOMICS (Steven N. Durlauf & Lawrence E. Blume eds., 2d ed. 2008); Daniel McFadden, *Conditional Logit Analysis of Qualitative Choice Behavior*, *in* FRONTIERS IN ECONOMETRICS 105 (Paul Zarembka ed., 1974); Pavlo R. Blavatskyy & Ganna Pogrebna, *Models of Stochastic Choice and Decision Theories: Why Both Are Important for Analyzing Decisions*, 25 J. APPLIED ECONOMETRICS 963 (2010); Drew Fudenberg & Tomasz Strzalecki, *Recursive Stochastic Choice* (Dec. 18, 2012) (unpublished manuscript), http://scholar.harvard.edu/?fudenberg/files/recursive_stochastic_choice.pdf.

89 Logit models are the most frequently used type of model in estimating a probability distribution of outcomes by a decisionmaker making a binary decision, such as whether or not to engage in an information flow. That model postulates that the probability distribution of a binary random variable Y_i, which takes the values 0 and 1, given the covariate X_i, is given by $\Pr(Y_i = 1 \mid X_i) = \exp(X_i \beta) / (1 + \exp(X_i \beta))$, where β is a parameter that determines the width of the curve. *E.g.*, Magnac, *supra* note 88. If we take Y_i to be the decision to engage or not in the information flow, with 1 corresponding to a decision to engage in the information flow, then X_i can be taken to represent a function of the relative private costs and benefits of the information flow, such as $X_i = (Benefit_i - Cost_i) / Cost_i$.

90 When $Benefit_i = Cost_i$, $X_i = 0$ and $\Pr(Y_i = 1) = \exp(0) / (1 + \exp(0)) = 1/2$.

relative to the costs, the probability that the information flow will occur approaches 100%, while as the costs increase relative to the benefits, the probability approaches 0%.

This stochastic-choice approach is a plausible description of the real world. Consider a shopping mall trying to decide whether to install a location-tracking system like the FootPath system discussed in the Introduction. If the cost of the system is $3 million and the best estimate of the present value of the system's benefits is $2.7 million, then the classical rational-choice model tells us that the mall will not install the system. Yet it is not hard to tell a story in which the mall decides nevertheless to go forward with the system. Maybe the mall operator is a risk-taker and values the upside potential more than the downside risks. Maybe the benefits are uncertain enough that the mall operator wants to run an experiment to see if they prove worthwhile.[91] Maybe the mall operator has simply miscalculated the costs and benefits. Regardless of the reason, it is plausible to think that rather than being 0%, the probability that the decisionmaker will decide to install the system might be closer to 20% or 30%. Yet if the best guess of the benefits was closer to $300,000 than $2.7 million, that probability might be far closer to 0%, since the cost would dominate the decisionmaking process.[92]

C. Aggregated Information Flows

Although both the rational-choice and stochastic-choice models offer plausible accounts in different circumstances of the decision to engage or not in an information flow, they are not enough to predict how often an information subject will be subject to invasions of privacy. To do so, we need to consider both the likelihood that a particular information flow will occur and how often such information flows have an opportunity to occur. Even an unlikely privacy loss can be a big problem if there are many opportunities for it to occur.[93]

This calculation ends up comporting with a wide variety of real-world intuitions about privacy. Take the example of a family building a home. The family might care about how much privacy the home will give them, but that is likely to be just one of numerous competing values, such as construction

91 Indeed, this is what happened in real life: Forest City, a large real-estate developer with numerous malls, installed the system in two of its properties as a test. *See* Censky, *supra* note 1.

92 Using the numbers in this example and the model given above, when the expected cost is $3 million and the expected benefit is $2.7 million, the covariate X_i, representing the relative costs and benefits of the project, is equal to –0.11. Setting the parameter $\beta = 10$, we get a probability of the information flow occurring of $\Pr(Y_i = 1) \approx 24.8\%$. If the expected benefit is $300,000, however, then $X_i = -9.0$, and $\Pr(Y_i = 1) \approx 0.00\%$.

93 To put it in the math of footnote 89, we can calculate the expected number of invasions of privacy over a time period by summing the individual probabilities of an invasion: $E(Y \mid X_i) = \Sigma_i (\exp(X_i \beta) / (1 + \exp(X_i \beta)))$. The value of this summation will increase with more terms in the summation, i.e., more opportunities for an invasion to occur.

and maintenance costs, energy efficiency, aesthetics of the home, views from the home, and so forth. A key design choice the family will face will be how many windows, and of what size, to include in the home. Larger windows make it easier for passers-by to observe the family's activities.[94] All else being equal, the family will have more privacy if they reduce the number and size of the home's windows, or increase the cost of invading privacy by using countermeasures like curtains. But all else is not equal; many more potential invaders will pass by if the home is in Manhattan than if it is in the middle of the woods. The family might have far more privacy in the woods, even in a home built like Johnson's Glass House or van der Rohe's Farnsworth House, than it would in an urban home with tiny windows.

This is a purely descriptive model, focusing on what information is collected, used, and disseminated by others, rather than on what the content of that information is. Though it ignores the sensitive or secret nature of any particular information flow, such a descriptive model is nevertheless useful, both because some areas of the law depend only on whether information is known to others, not on what that information is, and because it helps provide a roadmap for government regulation of privacy. The next Part develops that account.

III. Toward a Roadmap for Regulating Privacy

Ultimately, people who care about privacy should care about how it is regulated by the government. Designing effective privacy regulations is a surprisingly difficult problem, because naïve solutions like just maximizing or minimizing the amount of privacy information subjects enjoy are rarely the right answer. Privacy almost always requires tradeoffs. Give the police too much authority to peer into private affairs and you sacrifice privacy and liberty; but give too little and you sacrifice security and safety.[95] Moreover, these tradeoffs are dynamic: norms, technologies, and incentives change quickly, making it hard for law to keep up.[96] It is easy, then, for privacy regulations to have unexpected and unintended consequences.

This part takes the unilateral-invasion account of privacy developed in Part II and argues that it can help develop effective privacy regulations. It first addresses a necessary precondition: that normative privacy preferences look, at least in many contexts, to outcomes—to how easily information can be collected, used, and disseminated, or how often such information flows occur—rather than to absolute rights. It then uses the unilateral-invasion account to explain how law can best produce normatively desirable levels of privacy. Changes in norms, technologies, and incentives can alter a decisionmaker's cost-benefit analysis even when the optimal level of privacy has

94 In the language of the model, they reduce the cost of invading privacy, increasing X_i.

95 *Cf.* Jeremy Waldron, *Security and Liberty: The Image of Balance*, 11 J. Pol. Phil. 191 (2003).

96 *See* Kerr, *supra* note 13, at 485–87.

not changed, or has changed in a way that is inconsistent with the decisionmaker's costs and benefits. Law, then, can counteract these changes and restore the optimal level of privacy. Indeed, legal changes have followed this pattern in numerous domains. Finally, this Part addresses the most significant critique: that law should seek to give information subjects more control, or change who makes decisions about which information flows occur, rather than target unilateral invaders' incentives. Although such a strategy is promising in some contexts, it is likely to be unworkable most of the time, since the costs it would impose on information subjects would be prohibitive.

A. Outcome-Oriented Privacy

Privacy preferences take many forms; indeed, how to think normatively about privacy is one of the central debates in the field. Broadly speaking, normative views of privacy fall into two camps, which we can think of as behaviorist and consequentialist. The behaviorist camp looks to actors' actions rather than the consequences of those actions. Someone in this camp might assert, for instance, that individuals have the right to engage in certain actions due to the nature of those actions—to engage in a specific type of information flow, for instance, or to prevent that information flow from occurring. The First Amendment is a good example: with limited exceptions, the press has the right to publish whatever information it desires, including personal information, without the information subject's consent and regardless of the consequences of the publication.[97] It can also work the other way. Under right-of-publicity laws, for instance, individuals typically have the ability to block commercial uses of their likenesses.[98] Similarly, under the FTC's Do Not Call Registry, a phone user can prevent telemarketers from calling a given phone number.[99] These laws may or may not be designed with privacy in mind, but the key point is that an action can have privacy consequences—increasing or reducing an individual's privacy—even though the laws governing that action may be viewed as normatively desirable or undesirable without considering those consequences.

The consequentialist camp, in contrast, looks to the outcome of a given action and its effects on privacy rather than to the action itself. This camp focuses on how much privacy people have or what information is public or private. One good example is the context-sensitive ways in which police departments often release crime information. The Reno Police Depart-

97 *See, e.g.*, Florida Star v. B.J.F., 491 U.S. 524, 541 (1989) (holding that it violates the First Amendment to subject a newspaper to damages for publishing truthful, legally acquired information).

98 *E.g.*, White v. Samsung Elecs. Am., Inc., 971 F.2d 1395 (9th Cir. 1992), *reh'g denied*, 989 F.2d 1512 (9th Cir. 1993) (holding that a TV ad with a robot designed to look like Vanna White, flipping letters on a replica of the *Wheel of Fortune* game board, infringed White's exclusive right of publicity in her likeness).

99 *See* Do-Not-Call Implementation Act of 2003, 15 U.S.C. §§ 6151–55 (2012); *National Do Not Call Registry*, FED. TRADE COMM'N, https://www.donotcall.gov/ (last visited Jan. 29, 2016).

ment's media guide, for instance, explains the different kinds of information about the identities of criminal suspects and victims that may or may not be released. Arrestees' names are usually released, while victims' names are generally not released unless they are deceased and the next of kin has been notified.[100] In cases involving sexual offenses or crimes involving children, however, even the names of arrestees, and other information about the crimes, may not be released if it would tend to identify the victims.[101] Whether the Department engages in an action—releasing information about a crime—depends, then, on the privacy consequences of the information flow rather than anything about the action itself.

Consequentialist views of privacy are especially common in the criminal-procedure context, in which the Fourth Amendment's reasonableness framework invites a balancing of interests on each side. Indeed, Orin Kerr has argued that the Supreme Court's Fourth Amendment jurisprudence is best understood as a series of equilibrium adjustments, dynamic tweaks to the rules in response to exogenous changes. Under this theory, rule changes can be desirable because they give the government an approximately consistent level of access to investigatory information; consistency in the rules is less important than consistency in the privacy (or investigatory) consequences of those rules.[102] Under consequentialist views of privacy, then, the normative desirability of a law is a function of its privacy consequences, of the types and quantities of privacy it produces.

In many areas of the law, if privacy is a salient normative consideration—if we care about privacy as a relevant value—then we should judge the desirability of a law on consequentialist grounds rather than behaviorist, for two major reasons. First, many privacy harms arise out of downstream consequences of actions, rather than out of the actions themselves; a view of privacy that looks only to actions misses these harms. When a celebrity is harassed by a paparazzo seeking to take an unflattering photograph, for example, the mere act of taking the photo presumably causes its subject to feel some privacy loss: it might make him or her feel insecure and unsafe, as if there was no safe place to let his or her guard down.[103] But much of the harm stems from later publication of the photo, which can subject the target to ridicule, loss of income, and other consequential harms.[104] These consequential harms are especially pronounced in the kinds of privacy losses suffered by ordinary individuals. When a credit card processor suffers a data breach, for instance, the harms consist of things like fraudulent charges,

100 Reno Police Dep't, Media Guide 4–5 (2012), http://www.reno.gov/home/showdocument?id=42148.

101 *Id.* at 5.

102 *See* Kerr, *supra* note 13, at 526–29; *see also* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L.J. 213 (2002).

103 Ryan Calo classifies these harms, which arise out of the feeling of unwanted observation, as subjective privacy harms. *See* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 Ind. L.J. 1131, 1142–55 (2011).

104 *See id.* at 1147–55 (discussing objective privacy harms).

costs from having to update payment information for recurring charges, and maybe identity theft.[105] An analysis of processors' data-security measures that failed to consider those consequences is unlikely to come to the right balance of security and cost. Considering consequential privacy harms, then, is necessary to avoid missing a large part of the privacy story in a given field.

The second reason to prefer consequentialist views of privacy is that they better account for the factors that influence privacy outcomes. The effect of an action on privacy is not determined solely by the action; other, independent factors also play a role. The privacy effect of a paparazzi photo, for instance, depends not only on what the photo shows, but on how widely it spreads—and that might depend on the photographer's relationship with tabloid editors, the other things that happened that week and would compete for attention, and even whether Twitter or *The Daily Show* exist to help the photo go viral. And these factors are not stable; they change as norms, technology, and incentives change. A policy designed according to a behaviorist view of privacy, then, would have unpredictable effects, since changes to the broader context of an action would lead to changes in its privacy consequences. For instance, a policy providing that police have the right to track individuals' movements through space has strikingly different privacy consequences before and after GPS tracking devices become available.

Privacy is obviously not the only important value; there are numerous other reasons to support or oppose any given public policy.[106] I am not arguing that all public-policy decisions should be based on privacy consequences. Rather, the point is that when privacy matters, the best way to account for privacy is to analyze the consequences of a policy rather than the actions that lead to those consequences. Thinking of privacy in this way, as a set of consequences of information flows rather than a set of rights enjoyed by information subjects, makes it easier to design policies that produce desirable privacy consequences.

B. Regulating the Costs and Benefits of Information Flows

So what is the role of law in regulating privacy? As discussed in Part II, the amount of privacy enjoyed by an information subject is a function of what information flows occur, which in turn are, in many cases, unilaterally determined by outsiders. So it is those outsiders' incentives that need to be considered and, in many cases, adjusted. The trick is knowing when and how to

105 Data breaches have become increasingly common, as more and more information moves online and as criminals use security flaws to gain access to valuable information. *See generally* Kimberly Kiefer Peretti, *Data Breaches: What the Underground World of "Carding" Reveals*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 375 (2009); Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007); Caroline C. Cease, Note, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395 (2014).

106 Nor is privacy independent of these other values; there are often nonobvious interdependencies between privacy and other values. *See, e.g.*, Ryan Calo, *Privacy and Markets: A Love Story*, 91 NOTRE DAME L. REV. 649 (2015).

adjust those incentives, which requires a four-step process: (1) Identify a relevant normative privacy framework that applies in a given circumstance or set of circumstances and the information flows that should occur under that framework. (2) Identify the applicable decisionmakers who determine whether those information flows occur and the private costs and benefits they enjoy due to those information flows. (3) Compare the information flows that should occur according to the decisionmaker's cost-benefit analysis to those that should occur according to the relevant normative framework, identifying any mismatch between the decisionmaker's incentives and the normative ideal. (4) Use law to change the decisionmaker's cost-benefit analysis so it matches the relevant normative framework.

The first step, identifying a normative privacy framework, is where much of the hard work is done. The full range of possible frameworks is beyond the scope of this Article; law can play the same role to adjust incentives to match essentially any consequentialist privacy framework. Normative frameworks will vary greatly depending on the context, the participants' identities, the privacy interests at stake, and countless other factors. But we can imagine some frameworks that might obtain consensus among policymakers or other stakeholders. In the criminal-procedure context, for instance, we might think that in order to further society's interest in solving serious crimes, police investigating those crimes should be able to track suspects' movements in public. When investigating less-serious crimes, however, we might think that individuals' privacy interests outweigh society's interest in enforcing the law. Or, in the medical context, we might think that patients should be protected from embarrassment when receiving essential treatments, to avoid discouraging patients from seeking care, but that the privacy interests are less critical when patients get cosmetic work done. These might not be the best normative frameworks, but the point is that in each case, we want some information flows to occur more often and others to occur less often.

Once we have identified a normative privacy framework, we can move to the second step, identifying the applicable decisionmakers and their costs and benefits. In many cases, this will be straightforward. Police, for instance, are often the sole decisionmakers deciding whether to track a suspect's movements, though in some cases, technological barriers may require cooperation from someone else, like a telephone company or other business.[107] Sometimes the inquiry will be more complicated; for instance, patients, doctors, hospitals, and insurance companies influence what medical information is distributed to the public, but so do tabloid newspapers and other journalists

107 In many cases, courts or other legal officials will also be applicable decisionmakers, as when an officer is required to obtain a warrant before executing a search. We can disregard for now, however, these effects of legal rules, since the point of the exercise is to figure out how law can adjust the costs and benefits the applicable decisionmakers would face in the absence of legal rules.

who decide what information is worth publishing.[108] Regardless, understanding who the relevant decisionmakers are is important, since otherwise, policies that are intended to affect information flows may miss the mark.

The third step requires comparing the information flows that should occur in view of the relevant decisionmaker's cost-benefit analysis to those that should occur according to the normative framework identified in step one. This tells us whether any intervention is needed in the first place; if existing incentives are already producing the correct mix of information flows, then there is no problem to be solved. Only when the relevant decisionmaker's incentives produce the "wrong" information flows does law have any corrective role to play.

This point may seem uncontroversial, but it is not how policymakers and scholars usually think about privacy law. Under the unilateral-invasions theory, how much privacy individuals should enjoy in a given class of information—whether due to the sensitive nature of the information, the individuals' status, or any other factor—may be completely unrelated to how much the law should protect that privacy interest. And we see that in the real world: some things that can be highly sensitive—like information about individuals' sexual interests and activities—are legally unprotected. Existing incentives are strong enough to adequately protect this category of information, both because there are strong norms against trading this information, and because the relevant decisionmakers are usually limited to an individual and his or her sexual partners, who can decline to release information they want to keep private. Law would have little role to play. In other areas, sensitive information is legally protected precisely because there is a need; the Health Insurance Portability and Accountability Act, for instance, is needed to protect the privacy of health information because there are outsiders—health professionals—with access to sensitive information and incentives to use it.[109] Conversely, there are areas where there is no legitimate privacy interest—like disclosure of financial conflicts of interest by lawyers, doctors, and other fiduciaries—where law plays a privacy-*reducing* role. In these cases, without a legal rule, information would be *under*-disclosed; information about conflicts

108 For instance, after Mark Chanko's death was broadcast on the ABC documentary series *NY Med*, his family sued ABC, NewYork-Presbyterian Hospital, and the treating physician, Dr. Sebastian Schubl. Producers had blurred the video of Mr. Chanko, but his voice was audible and friends and family were able to identify him. *See* Charles Ornstein, *Dying in the E.R., and on TV Without His Family's Consent*, N.Y. TIMES (Jan. 2, 2015), http://www.nytimes.com/2015/01/04/nyregion/dying-in-the-er-and-on-tv-without-his-familys-consent.html. The lawsuit was dismissed, on the grounds that the producers' conduct "was not so extreme and outrageous as to support a claim for intentional infliction of emotional distress," and that no "personal information" was disclosed when the producers had blurred Mr. Chanko's face. *See* Chanko v. Am. Broad. Cos. Inc., 997 N.Y.S.2d 44 (N.Y. App. Div. 2014).

109 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, 2033–34 (codified at 42 U.S.C. §§ 1320d-2, 1320d-2, 1320d-4 (2012)); *see also* 45 C.F.R. §§ 164.500–.534 (2014) (codifying the privacy regulations).

of interest would be *too* private under existing norms, technologies, and incentives.

After identifying any mismatch between the information flows that should occur and those that are expected to occur, the fourth and final step is to design laws to bring the two into alignment. Since it is the relevant decisionmaker's cost-benefit analysis that determines which information flows occur, this is done by adjusting those costs and benefits. This can mean increasing or decreasing the costs of an information flow, or increasing or decreasing its benefits; all four possibilities must be considered.

There are innumerable ways to adjust the costs, to the relevant decisionmakers, of information flows. If the government wants to increase the cost of a class of information flows, for example, it can impose a tax or fee on it, as the British government did to newspapers under the Stamp Act[110] and does to television owners under the Television Licensing Regulations,[111] or as federal courts do when they charge fees for electronic access to court records,[112] or as copyright law does when it imposes statutory royalties for distributing cover songs.[113] Or law can ban a category of information flows outright (which then imposes legal costs for engaging in the information flow), as is done with child pornography,[114] for example, or with the use of certain medical information for marketing purposes.[115] Law can also impose indirect costs. When a business wishes to make use of customer information, for example, the law can impose disclosure or opt-in requirements, which impose compliance costs (from having to inform customers of the use) or reputational costs (from privacy-sensitive customers who disapprove of the use). Reducing the costs of information flows can take the opposite form, as when government provides subsidies, tax benefits, or prizes, or acts as a purchaser in the marketplace.[116] It can also provide infrastructure that supports information flows, as when the Defense Advanced Research Projects Agency, a piece of the Defense Department, created the computer networks that became the Internet.[117] And it can provide legal immunities that reduce the risk of engaging in information flows, as in Section 230 of the Communica-

110 *See* RANDALL P. BEZANSON, TAXES ON KNOWLEDGE IN AMERICA 13 (1994).

111 *See* Communications Act, 2003, ch. 21, §§ 231–40 (Eng., N. Ir.).

112 *See Electronic Public Access Fee Schedule*, U.S. COURTS (Aug. 20, 2014), http://www.uscourts.gov/services-forms/fees/electronic-public-access-fee-schedule.

113 *See* 17 U.S.C. § 115(c) (2012).

114 *See* 18 U.S.C. §§ 2252(a), (b)(1) (2012).

115 *See* 45 C.F.R. §§ 164.501, 164.508(a)(3) (2014).

116 Many of these activities are directed at generating new information, rather than at encouraging the collection, use, and disclosure of existing information. *See, e.g.*, *Challenges*, CHALLENGE.GOV, https://www.challenge.gov/list/ (last visited Jan. 29, 2016) (compiling government prizes for the development of new innovations). Still, the two mechanisms are the same. For instance, the tax exemption for religious institutions has the effect of subsidizing the dissemination of religious information—a subsidy for a specific category of information flows. *See* 26 U.S.C. § 501(c)(3) (2012).

117 *See, e.g.*, JANET ABBATE, INVENTING THE INTERNET 37, 185 (2000); KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET 10 (1996).

tions Decency Act, which immunizes providers of online services from liability for content posted by users of those services.[118] These are just some of the myriad tools the law has to adjust the costs of information flows; many others could be imagined as well.

Though it is harder than adjusting costs, there are also ways to adjust the benefits of a class of information flows. One way to do that is by adjusting the available alternatives to the information flows. This is especially true for business benefits of information flows, since many are available only because businesses have limited alternatives to achieve the same benefits. Businesses rely on information to focus their marketing efforts on the most likely customers, for example, but the benefits of doing so would be lowered if there were other effective marketing channels that did not rely on obtaining and using personal information. There is not always a clear line between adjusting costs and adjusting benefits; building the Internet, for example, created a communications infrastructure that reduced the cost of many information flows, but it also created network effects that increased their benefits. But regardless, the point is that costs and benefits are adjustable in numerous ways.

It is important to note that this is a dynamic process. As technologies, norms, and incentives change, the expected information flows will change with them. Unless normative privacy frameworks change in corresponding ways—and there is no good reason to think they will—law has to adjust to keep up. So, as new technologies made it easier and cheaper for police to monitor a suspect's movements in public, as happened in *United States v. Jones*,[119] more police took advantage of those new technologies to extend surveillance to more and more suspects. If the previous level of surveillance, which extended only to suspects in serious crimes, was the normatively ideal level, then the law needed to adjust to make it harder for police to use the new surveillance technologies. This is not the only possibility; maybe the correct normative view would permit broad surveillance, which was just impossible before due to technological limitations, or maybe the normative ideal shifted, say, after the September 11 attacks. But if the previous behavior was consistent with our normative privacy framework, and that framework did not change, then law needed to change to keep up with the new technologies—as, indeed, it did in *Jones*.

Many of these legal rules would have effects that go beyond those on individuals' privacy. A legal rule that results in the ideal set of information flows from a privacy perspective might have other effects that make it a bad idea, or just make it difficult or impossible to implement. But since there are so many ways to adjust the costs and benefits of information flows, it is likely that in most contexts there will be at least one solution that both improves privacy outcomes and has positive or neutral non-privacy effects. The chal-

118 *See* 47 U.S.C. § 230(c) (2012).

119 132 S. Ct. 945 (2012); *see also supra* text accompanying notes 11–12.

lenge of making policy is finding that balance, but the unilateral-invasion theory should help policymakers consider all the alternatives.

C. Regulating Unilateral Invaders

There is an important alternative strategy for policymakers looking to address privacy problems: work to make information flows more transparent and give information subjects the power to control how information about them is collected, used, and disseminated. Many privacy regulations and government recommendations take this approach, and it is a preferred strategy of most industries that use information about others.[120] At first glance, this strategy might seem better than the strategy of adjusting outsiders' costs and benefits, as described in Section III.B, since it tackles directly the problem of unilateral invasions by returning the decisionmaking power to information subjects instead of those outsiders. And when it works, it can have some significant advantages over strategies directed to outsiders. But in the majority of cases, it is likely to have significant downsides that make it unsuitable as a solution to most privacy problems.

Working to give information subjects more transparency and control over how information about them is collected, used, and disseminated has at least two significant benefits. First, it respects individual autonomy by giving individuals power over their own privacy. A society in which unilateral invasions are the norm could quickly become a society in which individuals have no expectations of privacy, and thus in which governments and corporations have greater control over even the most private aspects of people's lives. Returning control over how information is used can be a helpful first step toward seizing control over other aspects of people's lives from a distributed, decentralized Big Brother.

---

120 *See, e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 35–60 (2012) (recommending that businesses provide users with "simplified consumer choice"); THE WHITE HOUSE, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015 (2015) (focusing on transparency and consumer control as the cornerstones of a proposed privacy "bill of rights"); THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 11 (2012) (proposing that "[c]onsumers have a right to exercise control over what personal data companies collect from them and how they use it"). The FTC, for instance, is far more likely to take action against a company that violates its privacy policy than against one that follows a substantively unfair privacy policy. *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014). And in Europe, consent is the most common basis for data processing under the Data Protection Directive. *See* Council Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281/31) (adopting the Data Protection Directive); *Opinion of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data on 15/2011 on the Definition of Consent*, 01197/11/EN, WP 187, (July 13, 2011), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

And second, it better accounts for individuals' different privacy preferences. As Alan Westin showed, individuals have strikingly different feelings about privacy, with some caring deeply about privacy and others not caring at all.[121] The ideal normative privacy framework in many contexts may require respecting the privacy of individuals who place high value on privacy, but disregarding the privacy of those who do not care. We may want, for instance, to respect the privacy preferences of individuals who do not want to be tracked online by advertising companies, to provide an environment conducive to free expression and engagement with the community, while still using information about those who do not care about privacy so that online content can be supported economically. This requires a mechanism for soliciting and incorporating individual preferences, which might be easy to do if users have control over how information is used, and hard to do if regulation is directed toward outside invaders rather than information subjects.[122]

There are, nevertheless, reasons to be skeptical of efforts to give information subjects more transparency and control, at least as a strategy for solving privacy problems. Such strategies have been tried over and over, usually to little effect. Recall the complaints about the FootPath system, which tracked shoppers' movements through retail stores.[123] After Senator Schumer asked the FTC to intervene, he worked with seven major retail analytics companies to develop a voluntary industry code of conduct, under which companies agreed to allow consumers to opt out of tracking.[124] Yet so many things have to come true before a consumer opts out that it is almost inconceivable that more than a handful have done so: a consumer has to know that

121 Westin classified individuals into three categories: privacy fundamentalists, privacy pragmatists, and the privacy unconcerned. Privacy fundamentalists (who Westin estimated make up 25% of the population) "see[ ] privacy as an especially high value" and "reject[ ] the claims of many organizations to need or be entitled to get personal information for their business or governmental programs." Privacy pragmatists (55%) weigh privacy as a value but are willing to balance it against "the value, both to them and to society, of various business or government programs calling for personal information." And the privacy unconcerned (20%) not only do not worry about their own privacy, but don't see "what the 'privacy fuss' is all about" and don't understand why others would care. Alan F. Westin, *"Whatever Works": The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues*, *in* U.S. DEP'T OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997), http://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy#1F; *see also* PONNURANGAM KUMARAGURU & LORRIE FAITH CRANOR, PRIVACY INDEXES: A SURVEY OF WESTIN'S STUDIES (2005), http://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf; *see generally* ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

122 *See, e.g.*, Ariel Porat & Lior Jacob Strahilevitz, *Personalizing Default Rules and Disclosure with Big Data*, 112 MICH. L. REV. 1417, 1433–53 (2014).

123 *See supra* notes 1–8 and accompanying text.

124 *See* Carl Franzen, *Senator Unveils Plan to Restrict Tracking of Your Location Data in Retail Stores, Backed by Industry*, VERGE (Oct. 22, 2013, 7:19 PM), http://www.theverge.com/2013/10/22/4867952/NY-schumer-do-not-track-shoppers-retail-stores-self-regulating; *see also* FUTURE OF PRIVACY FORUM, MOBILE LOCATION ANALYTICS CODE OF CONDUCT (2013), https://fpf.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf; *Mobile Location Analytics Opt Out*, FUTURE OF PRIVACY FORUM (2014), http://smartstoreprivacy.org/.

retailers use such systems; has to hear about the opt-out system; has to find the site; and has to enter her phone's wifi and Bluetooth MAC addresses into the system.[125] Even then, she also has to remember to submit new MAC addresses any time she gets a new phone. And other opt-out systems have likewise had little uptake by consumers: few consumers opt out of receiving bulk mail; few consumers opt out of companies' sale of their information to outsiders for marketing purposes; and few consumers opt out of online tracking (whether through channels supported by tracking companies, through browser tools like the Do Not Track flag, or through plugins like Ghostery).[126]

There is a simple reason that opt-out rules do not work, and that other efforts give information subjects more transparency and control are unlikely to fare much better. The burden on individuals, who would have to make decisions about their own privacy in every privacy-relevant scenario, would be cost-prohibitive. Increasing the transparency of information collection, use, and disclosure, and increasing the control that individuals have, would surely reduce some of the costs of exercising that control. But it would not reduce those costs enough to allow individuals to exercise meaningful privacy choices for each and every potential privacy loss in their lives—every collection, use, and disclosure of information about an individual. Indeed, just considering the limited context of browsing the Internet, a 2008 study found that an average user would have to spend 201 hours a year, worth more than $3,500 per user, to read the privacy policy for each website he or she visited.[127] Adding in other contexts—other forms of communications, shopping in retail stores, transactions with financial institutions, education, health care, and so forth—would increase this number by much more. And Internet users have a relatively robust ability to control the collection of their

125 *See Mobile Location Analytics Opt Out*, *supra* note 124.

126 A notable exception is the FTC's Do Not Call registry, which lets consumers opt out of receiving unsolicited telemarketing calls. More than 200 million phone numbers have been registered in the system. *See* Lesley Fair, *10 Years of National Do Not Call: Looking Back and Looking Ahead*, FED. TRADE COMM'N: BUS. BLOG (June 27, 2013, 10:00 AM), http://www.ftc.gov/news-events/blogs/business-blog/2013/06/10-years-national-do-not-call-looking-back-looking-ahead. Possible explanations for the Do Not Call registry's atypical success include its extensive promotion and news coverage and the fact that it eliminates the hassle of receiving unsolicited calls, not just losses of privacy. Still, the success of the Do Not Call registry could provide useful lessons for those designing privacy-enhancing opt-out schemes. First, such schemes should be relatively simple. The Do Not Call registry, for example, requires only a phone number and an email address. Second, they should apply to a broad category of contacts after only one exercise of the right to opt out, rather than requiring individual actions for different invaders or different avenues of invasion. The Do Not Call registry, for example, applies to all commercial telemarketers, without requiring a user to act separately for each telemarketer. Third, opt-out schemes should be persistent, and should not require periodic maintenance. Phone numbers registered with the Do Not Call registry, for instance, do not expire, though the original version of the program required re-registration every five years.

127 Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 565 (2008).

personal information, through software tools and the ability to opt out of using certain services, compared to those in some other contexts. Even then, the simple cost of taking control can be so great that an information subject cannot reasonably exercise that control.

There are several reasons to think these costs would be difficult to surmount. First, the sheer number of potential privacy losses encountered by a typical person in a typical day is large, given the myriad contexts in which they arise and the myriad potential privacy invaders one might encounter. Repeat those options day after day after day, and a typical person would quickly become overwhelmed by sheer numbers.

Second, even if someone could make that many privacy decisions, many potential privacy losses are unknown to most people. It is a rare consumer who is likely to read the fine-print FootPath disclosure at a mall, or read about it in the press; the more likely scenario is that someone never even discovers that his or her cellphone might be tracked. Likewise, many consumers are unaware that governments and companies use license plate readers to build databases of cars' movements in public; or that outsiders track their activities online, let alone that more than a thousand companies do so. And disclosure mandates have a terrible track record of actually informing consumers of the things of which they are supposed to inform them.[128]

Third, even when someone knows about an information flow that can lead to a privacy loss, many such disclosures leave key terms vague, so that it is hard to know the privacy consequences of the information flow. The prototypical online privacy policy, for instance, discloses that information about a user may be used "to provide, maintain, protect[,] and improve" a company's services, without saying how the company does so, or what specific uses it makes.[129] Companies also routinely update privacy policies, introducing new terms without notice, other than by posting the new policy.

And fourth, even when a user knows how information may be collected, used, or disseminated, the future privacy consequences of that information flow are often unpredictable. They may depend on how technologies develop, how norms and incentives change, and even unpredictable changes like the sale of one company to another in bankruptcy.[130]

---

128 *See generally* BEN-SHAHAR & SCHNEIDER, *supra* note 67.

129 The example is from Google's privacy policy. *See Welcome to the Google Privacy Policy*, GOOGLE INC., http://www.google.com/policies/privacy/ (last modified Aug. 19, 2015).

130 *See, e.g.*, Bankruptcy Abuse Prevention and Consumer Protection Act of 2005, Pub. L. No. 109-8, § 231, 119 Stat. 23, 72–73 (codified as amended at 11 U.S.C. § 363(b)(1) (2012)) (restricting the sale in bankruptcy of personally identifiable information, when inconsistent with the debtor's privacy policy); Press Release, Fed. Trade Comm'n, FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000), https://www.ftc.gov/news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding (announcing a settlement after Toysmart.com, which had promised in its privacy policy not to share customer information with third parties, had offered its customer database as an asset for sale in bankruptcy proceedings).

Some contexts are better suited than others for strategies that aim to make information flows more transparent and give information subjects the power to control how information about them is collected, used, and disseminated. Such strategies may be more likely to work, for instance, when the underlying information flows are unusually important to the information subject, since in those circumstances it will be more worthwhile to spend the time and make affirmative privacy choices. But trying to extend those strategies to the myriad contexts in which information about individuals is collected, used, and disseminated is very likely a hopeless task.

Conclusion

Too often, accounts of privacy focus on information subjects, rather than outsiders who collect, use, and disseminate information. When privacy problems occur, these accounts suggest ways to give those information subjects more information about, and more control over, how information about them is collected, used, and disseminated. Yet, as this Article has demonstrated, this approach is often doomed to failure: it is usually the outsiders, not the information subjects, who decide whether an information flow will occur—and thus whether the information subject will enjoy more privacy or less. An information subject may or may not be aware of any given information flow, and even when aware, may have no influence over whether it occurs. Instead, in many cases the outsider chooses whether to commit a privacy invasion based on his or her incentives.

This model has important implications for the design of privacy regulations. Since, in many cases, the outside invader's incentives determine whether a privacy invasion will occur, effective privacy regulations are those that work to alter those incentives. This can be done by raising or lowering the private costs or benefits of a privacy invasion, to the outside invader, depending on how the other private costs and benefits of the invasion compare to the normative ideal. And since these costs and benefits change as norms, technologies, and incentives evolve, privacy regulations too must change to maintain the same level of privacy over time.