A TRADITIONAL TORT FOR A MODERN THREAT: APPLYING INTRUSION UPON SECLUSION TO DATAVEILLANCE OBSERVATIONS

BENJAMIN ZHU*

Dataveillance, a method of surveillance that collects and analyzes massive amounts of data about individuals, poses a threat to information privacy because it allows companies to uncover intimate personal information that individuals never consented to disclose. No comprehensive legal framework currently exists to regulate dataveillance. A potential remedy lies in the common law torts designed to protect privacy. However, the most applicable of these privacy torts, the tort of intrusion upon seclusion, faces several doctrinal hurdles in regulating dataveillance because courts and commentators consider the initial collection of data to be the only potential privacy intrusion from dataveillance. This Note proposes that the tort of intrusion upon seclusion could be updated to effectively regulate dataveillance if courts recognize that dataveillance's observation of new personal information constitutes its own privacy intrusion, distinct from the intrusion at the data collection stage. This doctrinal shift would overcome the doctrinal barriers to applying the intrusion upon seclusion tort to dataveillance.

* Copyright © 2014 by Benjamin Zhu. J.D., 2014, New York University School of Law; B.A. 2011, Northwestern University. I would like to thank Professor Catherine Sharkey for her essential guidance and encouragement. I am also grateful to Gabriel Ascher, Shayon Ghosh, Tom Gottheil, Steve Tensmeyer, and Michele Yankson for their feedback. Finally, I especially would like to thank Nikolaus Williams, Cristopher Santos, and the editors of the *New York University Law Review* for their hard work and careful editing. All errors are my own.

INTRODUCTION

"If we wanted to figure out if a customer is pregnant, even if she didn't want us to know, can you do that?" This was the question that Target's marketing department posed to an in-house statistician.[1] Because ingrained buying habits often change following the birth of a child, early knowledge of pregnancy would allow the retail chain to influence the parents' shopping preferences through personalized advertising.[2] The statistician's solution was a "pregnancy-prediction model" that could predict a customer's pregnancy status and due date within a small window of time.[3]

The statistician developed the model through data aggregation and mining, a process that compiles data and searches it for "implicit, previously unknown, and potentially useful information."[4] Target gathered vast amounts of data by assigning customers a unique identification number whenever possible to systematically track their purchase histories.[5] By analyzing the shopping habits of female customers in Target's baby shower registry, the statistician was able to observe how those habits changed as the women approached their due dates. The statistician used this information to build a computer program that assigned a "pregnancy prediction score" and an estimated due date to every female customer in its national database based on their purchasing patterns for twenty-five different products, including such mundane items as hand lotions, cotton balls, and dietary supplements.[6] Target developed a list of tens of thousands of women who were most likely pregnant, none of whom had consented to divulge that information. In one instance, a man who had received advertising for infant-related products confronted the manager of his local Target, accusing the company of encouraging his high school–aged daughter to get pregnant; he later learned that his daughter was in fact already

[1] Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES MAG., Feb. 19, 2012, at 30, 32, *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all.

[2] *Id.* at 33.

[3] *Id.* at 36–37.

[4] Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L. 74, 76 (2013) (citation omitted).

[5] Duhigg, *supra* note 1, at 33.

[6] *Id.* at 36–37. The customers in the database included women who had not signed up for the baby shower registry. *Id.*

pregnant.[7] While Target's actions may strike many to be intrusive and disturbing, the company insisted that it complied with all relevant federal and state laws.[8]

Such is life in the era of Big Data[9], an era when companies can "combine diverse digital datasets and then use statistics and other data mining techniques to extract from them both hidden information and surprising correlations."[10] Computer programs, perhaps even more sophisticated than Target's "pregnancy-prediction model," can be constructed from and applied to aggregated data to mine for still more personal information. This modern threat to privacy is known as "dataveillance," a term coined to describe methods of surveillance "not through the eye or the camera, but by collecting facts and data."[11] Potential sources of data concerning our daily lives abound, with "records [being] created about almost every facet of a person's life"[12] both by private actors[13] and governmental entities.[14] Collecting and analyzing these records is now a major business, with hundreds of companies dedicated to conducting dataveillance to uncover commercially useful information.[15]

Dataveillance allows companies to collect innocuous pieces of "unprocessed" data and generate them into intimate "processed" information about individuals, as Target did in turning receipts for

---

[7] *Id.* at 37.

[8] *Id.*

[9] *See* Steve Lohr, *The Age of Big Data*, N.Y. TIMES, Feb. 12, 2012, at SR1, *available at* http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?pagewanted=all (describing the growing impact of computer-assisted and data-driven analyses on modern life).

[10] Rubinstein, *supra* note 4, at 74.

[11] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 33 (2004); *see also* Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 270 (2008) (discussing how private companies conduct dataveillance by amassing databases of personal information collected online).

[12] SOLOVE, *supra* note 11, at 2.

[13] *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002) (describing maintenance of personal records by, among others, "Internet Service Providers (ISPs), phone companies, cable companies, merchants, bookstores, websites, hotels, landlords, [and] employers").

[14] *See* SOLOVE, *supra* note 11, at 127 (discussing the "smorgasbord of public records" covering one's existence from birth to death kept by federal, state, and local governments).

[15] *See id.* at 3–4 (describing companies, unknown to consumers, whose primary functions are aggregation and sale of data about consumers to marketers). For instance, Target could, and perhaps does, supplement its own customer records with data purchased from third parties or compiled in public records. The company could obtain customers' job histories, estimated salaries, reading habits, political leanings, divorce and bankruptcy proceedings, home addresses, and Internet browsing habits, and aggregate the data with its own purchase history records. Duhigg, *supra* note 1, at 33. For a discussion of the business of dataveillance, see *infra* Part I.A.

cotton balls into knowledge of its customers' pregnancy statuses.[16] This transformative power threatens the interest of information privacy, which holds that individuals should have control over the "acquisition, disclosure, and use" of their personal information.[17] Dataveillance undermines that control by allowing the discovery of personal information that individuals never consensually divulged.[18] Despite many proposals to safeguard against this modern threat to information privacy,[19] the dataveillance industry remains largely unregulated.[20]

A solution may lie in common law torts designed to protect privacy,[21] particularly the tort of intrusion upon seclusion.[22] This tort, also referred to as the intrusion tort, prohibits intentional intrusions, "physically or otherwise," upon the solitude, seclusion, or private affairs of an individual.[23] However, most commentators are pessimistic regarding tort law's ability to cope with modern privacy

---

16 *See* Rubinstein, *supra* note 4, at 76 ("Data mining enables firms to discover or infer previously unknown facts and patterns in a database. . . . [T]he newly discovered information is not only unintuitive and unpredictable, but also results from a fairly opaque process.").

17 Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1203 (1998).

18 *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 507 (2006) ("[A]ggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected."); Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 FORDHAM L. REV. 1731, 1734 (2006) ("[D]ata mining may compile a matrix of information about us more comprehensive and intimate than any intrusion into our homes . . . .").

19 *See, e.g.*, Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 358 (2006) (proposing legislative solutions for regulating commercial data brokers); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 242–43 (2013) (proposing solution based on increasing user access to data); Tal Z. Zarsky, *Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society*, 56 ME. L. REV. 13, 49 (2004) (proposing regulation on the use rather than collection of data); Nic Roethlisberger, Note, *Someone Is Watching: The Need for Enhanced Data Protection*, 62 HASTINGS L.J. 1793, 1797 (2011) (advocating for congressional action to regulate collection, use, sale, and theft of data).

20 *See* Rubinstein et al., *supra* note 11, at 273 ("[T]here is no comprehensive information privacy law in the US regulating private sector collection and use of personal data. . . . [N]either the Constitution nor a general set of laws regulates commercial companies' overall data practices as they affect privacy." (footnote omitted)).

21 *See* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1917–18 (2010) ("Sprouting from a law review article, [privacy torts] developed within a century into a well-established body of nationally-recognized law.").

22 *See id.* at 1919 (describing the intrusion tort as the "most likely candidate" to regulate dataveillance practices).

23 RESTATEMENT (SECOND) OF TORTS § 652B (1977).

threats.[24] This pessimism stems from courts and commentators who generally regard dataveillance to involve a privacy intrusion only at the stage of the initial collection of "unprocessed" data,[25] which complicates the application of the intrusion tort at a doctrinal level. First, the intrusion tort generally only protects matters that have been kept wholly secret, so collecting data voluntarily disclosed to third parties or available from public records is not actionable.[26] Second, the intrusion tort requires that the privacy intrusion be "highly offensive to a reasonable person" in order to be actionable.[27] This threshold is difficult to overcome because the pieces of data collected are generally innocuous when viewed in isolation.[28]

Despite these doctrinal difficulties, this Note proposes that the intrusion tort can and should be adapted to protect against abusive use of dataveillance. The tort *can* be adapted because, with the doctrinal shift recommended below, the tort's elements could be effec-

---

[24] *See* SOLOVE, *supra* note 11, at 58–59 ("The privacy torts . . . are not well adapted to regulating the flow of personal information in computer databases and cyberspace."); Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 330 (2013) ("The torts and their standards regarding information privacy are outdated and have not been adequately adapted to take into account new technologies and their effects on information privacy."); Richards & Solove, *supra* note 21, at 1919 ("The tort of intrusion, the most likely candidate to regulate the collection of information, faces several hurdles. Much of the compilation of data occurs from information . . . in the public domain, and courts have concluded that collecting such data is not an invasion into a person's 'solitude' or 'seclusion.'"); Roethlisberger, *supra* note 19, at 1798 ("[Intrusion upon seclusion] is unlikely to be applied more broadly [to protect personal information] because in most circumstances the user is giving up the information voluntarily."). While in the minority, a few commentators have proposed tort-based solutions for regulating modern privacy threats, although not the intrusion tort. *See* Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 146 (2006) (proposing a new common law tort to protect against data misuse); Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 69 (2003) (proposing a solution based on the tort of appropriation).

[25] *See infra* Part II (discussing the general application of the intrusion tort to the data collection stage of dataveillance).

[26] *See* Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1354 (Ill. App. Ct. 1995) ("We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation."); *infra* Part II.A (discussing the private-public dichotomy in privacy law). This approach reflects the common law's adherence to the "secrecy paradigm," which categorizes information as either "wholly private or wholly public." SOLOVE, *supra* note 11, at 143; *see also* Asay, *supra* note 24, at 330 ("Courts have . . . tended to adopt a binary view of privacy—some bit of information is either public or private—when in reality information is only rarely entirely public or private in the modern age; context matters."). For minor exceptions to the general rule, see *infra* note 105.

[27] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[28] *See* SOLOVE, *supra* note 11, at 59 ("Each particular instance of collection is often small and innocuous . . . . Indeed, courts have thrown out cases for intrusion involving the type of information that would likely be collected in databases.").

tively applied to dataveillance.[29] The intrusion tort *should* be adapted because alternative regulatory mechanisms have yet to be realized,[30] and there remains a need for a second-best solution to protect information privacy.

This Note argues that the tort of intrusion upon seclusion should recognize that dataveillance can cause multiple and distinct privacy intrusions—an initial intrusion at the stage of data collection and additional intrusions when data aggregation and mining result in the observation of personal information previously unrecognizable from the individual pieces of data collected. Applying the intrusion tort to the information observation stage of dataveillance rather than to the data collection stage would help ease the two doctrinal barriers discussed above. First, because the "processed" personal information observed through dataveillance may differ from the information revealed by the individual pieces of "unprocessed" data, the information being observed may still be considered secret even if the individual pieces of data were disclosed to third parties or made available in public records. Second, recognition that the observation stage constitutes a distinct privacy intrusion allows the offensiveness element of the tort to be assessed in light of the "processed" information uncovered by dataveillance, rather than based on the individual pieces of "unprocessed" data collected.[31]

This Note proceeds as follows. Part I elaborates on dataveillance's threat to information privacy. It also introduces the background and doctrinal elements of the intrusion tort. Part II discusses the difficulties presented by the current doctrinal framework, which applies the intrusion tort only to the data collection stage of dataveillance. Part III argues that dataveillance's information observation

---

[29] *Cf.* Kang, *supra* note 17, at 1262 ("[E]ven the generally limp common law privacy tort of intrusion upon seclusion has at times responded to new technologies of surveillance. On this view, cyberspace can be seen as the next gizmo that warrants response." (footnote omitted)).

[30] *See infra* notes 69–76 and accompanying text (discussing the lack of a comprehensive legal framework protecting information privacy from dataveillance).

[31] The privacy scholar Jane Yakowitz Bambauer has proposed a similar framework. *See* Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 209–10 (2012) (proposing "an expansion of the intrusion tort to fit the modern technological landscape"). She advocates that the intrusion tort should provide recourse for the observation of personal data if the observation would be highly offensive to a reasonable person, including for "machine observation[s]" occurring through dataveillance. *Id.* at 244–45. This Note concurs with much of Bambauer's insights and builds on her argument by providing greater doctrinal support for the adoption of such a framework. *See infra* Part III.A (providing doctrinal justifications for this Note's proposed framework). Nevertheless, it differs from Bambauer's assessment in several areas, including how to determine when dataveillance results in a potentially tortious observation. *See infra* Part III.B.1 (defining when a dataveillance observation may constitute a distinct privacy intrusion).

stage should constitute a distinct privacy intrusion. It justifies the proposal by examining case law on the intrusion tort and other fields of privacy law. It then elaborates on how this Note's proposed framework would ease the previously identified doctrinal obstacles and applies the framework to illustrative examples. Finally, it addresses some counterarguments to this Note's proposal.

I
Traditional Privacy Torts and Modern Privacy Threats

A. Dataveillance's Threat to Information Privacy

Target's "pregnancy-prediction model" demonstrates the ability of dataveillance to aggregate massive amounts of seemingly innocuous data and extract from them intimately revealing personal information.[32] And Target is far from the only company to engage in such practices. A multibillion-dollar industry has grown out of "database marketing," also known as "targeted marketing," which aims to use dataveillance to personalize the type of advertisements consumers receive based on their individual preferences.[33] Almost every major retailer employs in-house analysts to build complex algorithms that assess customers' preferences and optimize marketing strategies.[34] Beyond the in-house departments, dedicated database marketing companies collect massive amounts of data, conduct sophisticated analyses, and construct consumer profiles for sale to any interested parties.[35] The database of a single company, Acxiom Corporation, contains information on about 500 million active consumers worldwide—including a majority of adults in the United States—with approximately 1500 data points per consumer.[36]

---

[32] *See supra* notes 1–7 and accompanying text (describing the methodology of the "pregnancy-prediction model").

[33] *See* Solove, *supra* note 11, at 17–20 (discussing the industry of targeted advertising); Stan Karas, *Privacy, Identity, Databases*, 52 Am. U. L. Rev. 393, 399–400 (2002) ("Database marketing is currently the most promising form of marketing, growing at twice the rate of America's GNP."); Natasha Singer, *You for Sale: A Data Giant Is Mapping, and Sharing, the Consumer Genome*, N.Y. Times, June 17, 2012, at BU1 (describing database marketing as a multibillion-dollar industry).

[34] *See* Duhigg, *supra* note 1, at 33 ("Almost every major retailer, from grocery chains to investment banks to the U.S. Postal Service, has a 'predictive analytics' department devoted to understanding not just consumers' shopping habits but also their personal habits, so as to more efficiently market to them.").

[35] *See* Singer, *supra* note 33, at BU1 (discussing the scale of the database marketing industry).

[36] *Id.*

Companies use dataveillance for more than just marketing. Data aggregation and mining are used to assess credit risks and perform background checks.[37] Companies may also provide disparate levels of service to customers based on profiles compiled through data analysis.[38] For example, companies are beginning to use personal information to categorize individuals as "angel" or "demon" customers based on their expected degrees of profitability.[39] "Angel" customers may be given preferential treatment, while "demon" customers are turned away entirely.[40] Such practices raise concerns beyond those related to privacy and demonstrate the potential social consequences of dataveillance gone unchecked.

Vast amounts of private and public records supply the raw data on which dataveillance runs. The conveniences of the modern era require individuals to interact with various companies on a daily basis—Internet service providers, cable companies, phone companies, insurance companies, and more. All of these entities maintain records on their customers,[41] and few legal constraints exist to limit the use of the data being collected.[42] These databases of records constitute valuable assets in the age of Big Data, and companies may sell or rent their data to the highest bidders.[43] Moreover, the increasing digitalization of modern life—with user information recorded on computers, cell phones, and tablets—has compounded the availability and descriptiveness of data on every aspect of our lives.[44]

On the public side, federal, state, and local governments extract a wealth of personal information from the populace, much of which is placed into the public domain. Public records exist to keep track of people's marriages and divorces, political affiliations, professional and employment histories, property ownership, and contacts with law

---

[37] *See* SOLOVE, *supra* note 11, at 3 (discussing how companies use "digital dossiers," collections of detailed data about individuals, to assess creditworthiness and to conduct background checks).

[38] *Id.* at 50.

[39] *Id.*

[40] *Id.*

[41] *Id.* at 20.

[42] *See infra* notes 69–76 and accompanying text (discussing the patchwork of laws regulating information privacy).

[43] *See* SOLOVE, *supra* note 11, at 19 ("An increasing number of companies with databases—magazines, credit card companies, stores, mail order catalog firms, and even telephone companies—are realizing that their databases are becoming one of their most valuable assets and are beginning to sell their data.").

[44] *See id.* at 22–26 (summarizing how cyberspace has aided the collection, buying, and selling of personal information); *see also* Rubinstein et al., *supra* note 11, at 270 ("[P]rivate companies are now amassing and analyzing rich databases of personal information collected online.").

enforcement and the legal system.[45] These records present a treasure trove of personal information, some of which may be extremely sensitive and intimate.[46] Federal and state laws mandate that much of these records remain open to the public, and legal regulations on the use of personal information contained within them are patchy at best.[47] In the past, practical difficulties hindered the use, and misuse, of personal information found in public records. Public documents often only existed in physical form at a local government office, limiting their accessibility.[48] Today, government offices are increasingly placing public records online and requiring electronic filings.[49] The digitization of public documents allows private companies to "sweep up millions of records from record systems throughout the country and consolidate them into gigantic record systems."[50] Thus, the government has become another supplier of the fuel on which dataveillance feeds.

The degree of intrusiveness varies among dataveillance practices and the personal information they uncover. For instance, Pandora—the online music streaming service—may accurately predict an individual's musical preferences by analyzing data collected from its thousands of users, but few people are likely to find such a practice intuitively offensive.[51] On the other end of the spectrum, a Google executive has alleged that credit card companies can analyze spending patterns to identify with ninety-eight percent accuracy whether and when a married couple will divorce.[52] Perhaps even more unsettling, companies now employ dataveillance to uncover private medical information about individuals by aggregating and mining data on hundreds of variables, including age, race, premium cable subscription, "a preference for jazz," and cat ownership.[53] According to a pharmaceu-

---

[45] *See* SOLOVE, *supra* note 11, at 127–31 (detailing various public records that may contain personal information).

[46] *See id.* at 129–30 (discussing how court records, which are generally open to the public, may contain information such as medical data and Social Security numbers).

[47] *See id.* at 132–39 (summarizing regulations on disclosure and use of public records).

[48] *Id.* at 131.

[49] *See id.* (discussing the increased digitization of court records).

[50] *Id.*

[51] *See* Bambauer, *supra* note 31, at 246 (discussing the inoffensiveness of Pandora's retention of personal preferences).

[52] Oliver Burkeman, *SXSW 2011: The Internet Is Over*, GUARDIAN (Mar. 14, 2011, 4:00 EDT), http://www.theguardian.com/technology/2011/mar/15/sxsw-2011-internet-online. Credit card companies have denied that they monitor data to predict potential divorces. Nicholas Ciarelli, *How Visa Predicts Divorce*, DAILY BEAST (Apr. 6, 2010), http://www.thedailybeast.com/articles/2010/04/06/how-mastercard-predicts-divorce.html (noting Visa's denial of such a practice).

[53] Joseph Walker, *Data Mining to Recruit Sick People*, WALL ST. J., Dec. 17, 2013, at B1.

tical executive, lifestyle data such as credit card history and "whether you drive an American automobile" can be analyzed to obtain a "very, very close bead" on whether someone has a particular disease, thereby allowing companies to target the individual for marketing or clinical trials.[54] While stringent federal laws regulate the use and disclosure of personal medical information, dataveillance allow companies to circumvent those restrictions: Because the pieces of data being collected, aggregated, and mined are not subject to the relevant statutes, the observation of medical information through dataveillance falls outside of the laws' protection.[55]

Such aggressive forms of dataveillance threaten the interest of information privacy.[56] Information privacy concerns "an individual's control over the processing—i.e., acquisition, disclosure, and use—of personal information."[57] A paradigmatic violation of information privacy occurs when someone obtains medical information about another by looking through confidential files without permission.[58] However, information privacy does not only protect especially sensitive, private, or embarrassing information. Rather, "personal information" encompasses all information that is "identifiable to an individual."[59] This Note adopts Jerry Kang's broad conception of personal information, which holds that information can be identifiable to an individual in three ways: (1) The individual purposefully created or authored the information; (2) the information describes the individual in some manner; or (3) the information identifies the individual for some institutional or security purpose.[60] The first category includes telephone conversations, letters, and emails; the second category includes biometric facts (e.g., height, weight, blood type), biographical facts (e.g., birth date, sexual orientation, criminal history), and records of discrete actions (e.g., receipt proving a visit to a particular store to

---

[54] *Id.*

[55] *See id.* at B2 (discussing how federal privacy laws do not protect "the clues that people leave about their health outside of their medical records").

[56] Beyond the domain of the common law privacy torts, the protection of privacy has become the subject of constitutional law, evidentiary privileges, and various federal and state statutes. *See* Solove, *supra* note 18, at 483 (discussing various fields of American privacy law). Despite the ubiquitous use of the word "privacy," the term encompasses different interests, including "ideas of bodily and social autonomy, of self-determination, and of the ability to create zones of intimacy and inclusion that define and shape our relationships with each other." A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1466 (2000). This Note focuses on the interest of information privacy.

[57] Kang, *supra* note 17, at 1203.

[58] *Id.*

[59] *See id.* at 1206–07 (discussing the definition of personal information central to information privacy).

[60] *Id.* at 1207–08.

purchase a particular item at a particular time); and the third category includes Social Security numbers and ATM pins.[61] Thus, information privacy holds that individuals should have control over a variety of information about themselves, ranging from the sensitive to the trivial. Even consumer preferences deserve some protection under the broad conception of information privacy, as individuals' product and brand choices constitute part of their personal identities.[62]

Information privacy supports various normative values. Control over personal information may help avoid embarrassment, create social relationships, and prevent misuse of personal information,[63] while nonconsensual observation of personal information may infringe on human dignity and lead to self-censorship.[64] Comprehensive discussion of the benefits and costs of information privacy is neither feasible nor necessary here. For the purpose of this Note, it suffices to "assume that information privacy is a good in itself, and a value worth protecting, although not at all costs."[65]

To be sure, dataveillance provides significant societal benefits. The ability to uncover hidden patterns and facts from large collections of data has positively impacted fields ranging from national security to medical research to urban planning.[66] But it also may undermine information privacy. The goal, then, is to limit the privacy risks posed by dataveillance without stifling its positive utilities.[67]

Commentators note that purely private mechanisms are unlikely to reach such an ideal balance given the power and information imbal-

---

[61] *Id.*

[62] *See* SOLOVE, *supra* note 11, at 45 ("We have many choices in the products we buy, and even particular brands symbolize certain personality traits and personal characteristics."); Karas, *supra* note 33, at 394 (arguing that consumers' choices constitute part of their individual identities).

[63] *See* Kang, *supra* note 17, at 1212–17 (detailing how privacy serves the purposes of helping people avoid embarrassment, construct social intimacy by selecting who have access to their personal information, and maintain control and power in transactional processes).

[64] *See id.* at 1260 (arguing that information privacy protects human dignity); *see also* Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 223, 228–30 (Ferdinand David Schoeman ed., 1984) (arguing that "privacy might be grounded on the more general principle of respect for persons," which is violated by unwanted observations that affect the target's self-awareness and decisional autonomy).

[65] Froomkin, *supra* note 56, at 1467 (footnotes omitted).

[66] Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. ONLINE 25, 25 (2013), http://www.stanfordlawreview.org/sites/default/files/online/topics/PolonetskyTene.pdf.

[67] *See* Tene & Polonetsky, *supra* note 19, at 241 ("The extraordinary societal benefits of big data . . . must be reconciled with increased risks to individuals' privacy.").

ances present in the market.[68] The legal framework regulating dataveillance also remains lacking. While the importance of maintaining individuals' control over their private information has long been recognized under the law,[69] the United States lacks comprehensive statutory protection for information privacy.[70] Various statutes regulate the use of personal information by private entities, but they narrowly target specific industries and practices.[71] Moreover, while the federal government and all fifty states have passed freedom of information laws that provide substantial public access to government and other public records,[72] no uniform standard exists to control the use of personal information found in those records.[73] In sum, statutory protection of information privacy exists to some degree, but the patchwork of laws contains "significant gaps and omissions,"[74] including a lack of comprehensive regulation of dataveillance.[75] Target's "pregnancy-prediction model" and the use of dataveillance to identify individuals' medical histories—practices that may seem intuitively objectionable to many—are not covered by the current statutory

---

[68] *See* SOLOVE, *supra* note 11, at 81–87 (discussing limits to market-based solutions for protecting privacy rights).

[69] Official recognition of the need to protect information privacy is embodied in the Fair Information Practices (FIPs), a set of internationally recognized principles addressing the privacy of personal information. The FIPs were first proposed by a United States government advisory committee in 1973 and are now reflected in the privacy laws of various countries. *See* Robert Gellman, *Fair Information Practices: A Basic History*, BOBGELLMAN.COM, http://bobgellman.com/rg-docs/rg-FIPShistory.pdf (last modified Aug. 3, 2014) (providing history of FIPs and details of origins in 1970s).

[70] *See* SOLOVE, *supra* note 11, at 67 (noting that the United States does not have a comprehensive law protecting privacy in general).

[71] Covered industries include credit reporting agencies, cable companies, the medical industry, and financial institutions. *See id.* at 67–71 (summarizing various industry-specific, privacy-related statutes).

[72] *Id.* at 134–35.

[73] *Id.* at 138–39.

[74] *Id.* at 71.

[75] *See id.* ("[T]he federal statutes cover only a small geography of the database problem."); *see also* Karas, *supra* note 33, at 401 ("The lack of comprehensive laws protecting personal informational privacy in the United States has made database marketing possible."); Ludington, *supra* note 24, at 151 ("The current system—if it can be called one—for regulating the use of personal information by private data traders does so inconsistently and unpredictably."); Solove & Hoofnagle, *supra* note 19, at 357 ("[E]merging companies known as 'commercial data brokers' have frequently slipped through the cracks of U.S. privacy law."). The Obama administration has pushed for increased privacy protection against modern privacy threats, but its proposals focus on nonbinding principles rather than legislative action. *See generally* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (proposing a set of nonbinding principles regarding information privacy).

framework.[76] Given the inadequacies of the existing statutes and regulations, a second-best solution is needed to check abusive use of dataveillance. A potential candidate for filling the interstices lies in the common law tort of intrusion upon seclusion, which is discussed below.

B. History and Doctrine of Intrusion Upon Seclusion

As one federal judge stated, "[a]ll comment upon the right of privacy must stem from the famous article by Warren and Brandeis."[77] Annoyed by newspapers' intrusive reporting on his personal affairs, businessman Samuel Warren turned to his former law partner Louis Brandeis to help conceive of a remedy.[78] Examining various fields of common law, Warren and Brandeis extracted the general principle that an individual has a right to privacy.[79] This "right to be let alone"[80] protected against the "mental pain and distress" caused by the invasion of an individual's "solitude and privacy."[81] Warren and Brandeis viewed such protection to be more essential than ever in light of the technological advances fueling the growth of mass media.[82]

A subsequent law review article by Dean William Prosser defined the contours of the common law torts that had developed to protect privacy, giving them "order and legitimacy."[83] Examining the hundreds of court decisions that followed Warren and Brandeis in recognizing some common law right to privacy, Prosser distilled from them four distinct torts, including intrusion upon seclusion.[84] Prosser's definition of the intrusion tort was incorporated into the *Second Restate-*

---

[76] *See* Duhigg, *supra* note 1, at 37 (quoting a Target spokesperson insisting that the company complies with all state and federal laws); Walker, *supra* note 53 (noting that federal medical privacy laws do not apply to observing medical information through the use of dataveillance).

[77] Sidis v. F-R Pub. Corp., 113 F.2d 806, 808 (2d Cir. 1940).

[78] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 383 (1960).

[79] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213 (1890) ("The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to [other spheres]."); *see also* Prosser, *supra* note 78, at 384 ("Piecing together old decisions in which relief had been afforded on the basis of defamation, or the invasion of some property right, or a breach of confidence or an implied contract, the article concluded that such cases were in reality based upon [the] broader principle [of the right to privacy].").

[80] Warren & Brandeis, *supra* note 79, at 193.

[81] *Id.* at 196.

[82] *See id.* at 195 (citing "recent inventions and business methods" as bringing attention to the need to secure privacy); *see also id.* at 196 ("Of the desirability—indeed of the necessity—of some such protection, there can, it is believed, be no doubt. The press is overstepping in every direction the obvious bounds of propriety and of decency.").

[83] Richards & Solove, *supra* note 21, at 1888.

[84] *See* Prosser, *supra* note 78, at 389 (outlining the four distinct kinds of invasion).

ment of Torts,[85] which remains the primary authority on the subject for courts today.[86] Prosser's formulation of the intrusion tort, as codified in the Restatement, states in full: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[87]

Thus, although courts differ in the exact formulation, a tortious intrusion involves three elements: (1) The defendant intentionally committed an unauthorized intrusion, physically or otherwise; (2) the intrusion infringed upon the plaintiff's private seclusion, affairs, or concerns; and (3) the intrusion would be considered highly offensive to a reasonable person.[88] Recovery of damages also requires showing that the intrusion caused emotional or mental distress.[89]

The intrusion tort initially applied to undue physical intrusions, such as into one's home, hotel room, and personal items.[90] In such cases, the intrusion tort "overlap[s], to a considerable extent at least, the action for trespass to land or chattels."[91] However, courts soon applied the tort to nonphysical intrusions, such as "eavesdropping upon private conversations" and "peering into the windows of a home."[92] The Restatement's comments emphasize that the tort protects against such unwanted surveillance, even when no trespass occurs and the victim remains unaware of the conduct.[93]

---

[85] Prosser also served as the chief reporter for the Restatement (Second) of Torts. *See* Richards & Solove, *supra* note 21, at 1890 (describing how Prosser's formulation became the predominant one).

[86] *See* Andrew Jay McClurg, *Bringing Privacy Law out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N.C. L. REV. 989, 998–99 (1995) ("Courts in at least twenty-eight states have explicitly or implicitly accepted each of the four torts delineated by Prosser, almost always relying upon the *Restatement* definitions. . . . Virtually all states have recognized a tort cause of action for invasion of privacy in some form."). For a critical assessment of Prosser's influence on the modern state of privacy law, see Richards & Solove, *supra* note 21, at 1890, stating that "[a]lthough Prosser gave tort privacy order and legitimacy, he also stunted its development in ways that have limited its ability to adapt to the problems of the Information Age."

[87] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[88] *See* Wolf v. Regardie, 553 A.2d 1213, 1217 (D.C. 1989) (listing three elements of the intrusion tort).

[89] *See* Pulla v. Amoco Oil Co., 882 F. Supp. 836, 867–69 (S.D. Iowa 1994) (discussing degree of emotional distress necessary to sustain intrusion claim), *rev'd in part on other grounds*, 72 F.3d 648 (8th Cir. 1995); Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1354 (Ill. App. Ct. 1995) (listing "anguish and suffering" as element of intrusion tort).

[90] *See* Prosser, *supra* note 78, at 389 (noting various applications of intrusion tort).

[91] *Id.* at 390.

[92] *Id.*

[93] *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977) (explaining intrusion tort's applicability to purely sensory intrusion, such as wiretapping, eavesdropping, or

The intrusion tort's applicability to nonphysical intrusions is significant for at least two reasons. First, it indicates that the tort may be adapted to apply to the type of nonphysical privacy invasions caused by dataveillance, which involve the unwanted observation of personal information.[94] Second, it demonstrates that the tort already protects privacy interests beyond those secured by trespass-related torts, including information privacy. Indeed, even commentators skeptical of tort law's ability to deal with modern privacy threats point to the intrusion tort as the most viable common law solution for regulating dataveillance.[95] However, doctrinal impediments hinder the applicability of the intrusion tort. The next Part examines these obstacles and demonstrates that they arise from the exclusive application of the intrusion tort to the data collection stage of dataveillance.

II
Doctrinal Obstacles to Applying the Intrusion Tort to Dataveillance

Commentators express skepticism regarding the viability of the intrusion tort to protect against dataveillance's threat to information privacy.[96] Much of the skepticism is rooted in the view that the intrusion tort only applies to the privacy intrusion at the collection stage of the individual pieces of "unprocessed" data. This framework presents two doctrinal obstacles. The first obstacle is the line that privacy law draws between private and public spheres of activities, which Daniel Solove labels the "secrecy paradigm."[97] The second obstacle is the intrusion tort's demand that the privacy invasion be "highly offensive to a reasonable person," which this Note refers to as the offensiveness

peeking through upstairs window with binoculars); *see also* Nader v. Gen. Motors Corp., 255 N.E.2d 765, 770 (N.Y. 1970) (holding that unauthorized wiretapping and eavesdropping clearly constitute invasions of privacy); Prosser, *supra* note 78, at 390 (discussing nonphysical intrusions); Adam J. Tutaj, *Intrusion Upon Seclusion: Bringing an "Otherwise" Valid Cause of Action into the 21st Century*, 82 Marq. L. Rev. 665, 671 (1999) (listing "purely sensory invasion" as subject to the intrusion tort).

[94] *See infra* Part III.A (elaborating on the application of the intrusion tort to privacy invasions caused by observation of personal information).

[95] *See* Kang, *supra* note 17, at 1262 (noting that intrusion upon seclusion may be updated to respond to modern privacy threats); *see also* Richards & Solove, *supra* note 21, at 1919 (identifying the intrusion tort as the privacy tort most likely to apply to dataveillance).

[96] *See supra* note 24 (presenting examples of commentary pessimistic about tort law's ability to police dataveillance).

[97] Solove, *supra* note 11, at 42.

requirement.[98] This Part examines these doctrinal obstacles to the intrusion tort's applicability to dataveillance.[99]

A. The Secrecy Paradigm

The secrecy paradigm refers to the law's conception of privacy problems as involving "invasions into one's hidden world."[100] Under this framework, an individual maintains a privacy interest in information that has been kept secret, but that interest evaporates if the information is disclosed or made public. Once disclosed, the information becomes part of the public domain and is available for any use.[101] Prosser's formative definition of intrusion upon seclusion reflects the secrecy paradigm, stating that "[i]t is clear . . . that the thing into which there is prying or intrusion must be, and be entitled to be, private."[102]

Recall that a tortious intrusion involves (1) an intentional and unauthorized intrusion (2) that infringes upon the plaintiff's private seclusion, affairs, or concerns (3) that would be considered highly offensive to a reasonable person.[103] The first and second elements of the tort reflect the secrecy paradigm. The first element contemplates disclosure of information to a third party. A third party's surveillance of personal information is not *unauthorized* if the information has been voluntarily disclosed to that party.[104] Likewise, no unauthorized intrusion occurs if the third party passes the previously disclosed information on to another party.[105] The second element reflects the

---

[98] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[99] The case law in this area is scarce, possibly because of the aforementioned doctrinal difficulties. This Note does not discuss recent cases brought against Apple and Google for alleged privacy violations, which include claims of intrusion upon seclusion. These cases were dismissed from federal district courts for lack of Article III standing based on failure to identify concrete economic injuries from the alleged privacy harms. *See In re* Google, Inc. Privacy Policy Litig., No. C 12–01382 PSG, 2012 WL 6738343, at *5 (N.D. Cal. Dec. 28, 2012) ("Plaintiffs have not identified a concrete harm . . . sufficient to create an injury in fact."); *In re* iPhone Application Litig., No. 11–MD–02250–LHK, 2011 WL 4403963, at *4 (N.D. Cal. Sept. 20, 2011) ("[F]or purposes of the standing analysis under Article III, Plaintiffs' current allegations are clearly insufficient."). These cases may indicate the difficulty of establishing *damages* from a dataveillance privacy intrusion, but they do not negate this Note's argument that dataveillance can result in tortious intrusion *liability*.

[100] SOLOVE, *supra* note 11, at 42.

[101] *See id.* at 143 (discussing the "black-and-white" line between public and private information).

[102] Prosser, *supra* note 78, at 391.

[103] *Supra* note 88 and accompanying text.

[104] *See* Johnson v. Stewart, 854 So. 2d 544, 549 (Ala. 2002) ("A wrongful-intrusion claim cannot be based upon information voluntarily given to the defendant by the plaintiffs . . . .").

[105] *See id.* at 549–50 ("A wrongful-intrusion claim cannot be based upon . . . the defendant's receipt of information already known to others."). The application of the secrecy paradigm in this situation may be justified under a consent rationale: One consents

lack of privacy interest in information available to the public at large. Surveillance of activities conducted in public generally does not intrude into a *private* affair,[106] and thus "public information . . . cannot form the basis for an invasion-of-privacy claim."[107]

The secrecy paradigm's focus on the private-public dichotomy hinders the application of the intrusion tort to the data collection stage of dataveillance, which generally involves the collection of data available from third parties or public records.[108] Under the secrecy paradigm, individuals lack a privacy interest in such data.[109] Thus, the intrusion from the collection or use of such data would not be *unauthorized* or infringe upon a *private* concern.

---

to the risk that the third party to whom information had been disclosed will engage in further dissemination of that information. Thus, secretly wiretapping or recording a phone conversation without the consent of either party to the conversation constitutes an intrusion upon seclusion, while identical conduct by, or with the consent of, an involved party does not violate privacy. *Compare* Milke v. Milke, No. 03–CV–6203 JMR/FLN, 2004 WL 2801585, at *1, *4–5 (D. Minn. June 14, 2004) (granting summary judgment for intrusion upon seclusion claim based on a secret recording of a phone conversation without consent of either party to the conversation), *and* Rhodes v. Graham, 37 S.W.2d 46, 47 (Ky. 1931) (allowing invasion of privacy claim based on wiretapping without consent of any participants in the conversation), *with In re* Bates, 555 S.W.2d 420, 430–31 (Tex. 1977) (finding no invasion of privacy when a party to phone calls taped the conversations and turned them over to police).

106 *See* Solove, *supra* note 18, at 498 ("[P]laintiffs bringing claims involving surveillance in public have generally not been successful."); *see also* Muratore v. M/S Scotia Prince, 656 F. Supp. 471, 482–83 (D. Me. 1987) (rejecting intrusion claim when photographers harassed plaintiff in public places, because tort requires "intrusion into a physical realm that is uniquely the plaintiff's"), *vacated in part on other grounds*, 845 F.2d 347 (1st Cir. 1988). However, a few courts have been willing to recognize an intrusion upon seclusion when the offensive activities occurred in a public setting but extreme circumstances existed. For example, in *Nader v. General Motors Corp.*, 255 N.E.2d 765 (N.Y. 1970), the court held that an issue of fact existed as to whether extremely close surveillance of the plaintiff as he withdrew money in a bank constituted an actionable intrusion even though the surveillance occurred in a public place. *Id.* at 771. In so holding, the court stated that while "mere observation of the plaintiff in a public place does not amount to an invasion of his privacy," in some circumstances "surveillance may be so overzealous as to render it actionable." *Id.* (quoting Pearson v. Dodd, 410 F.2d 701, 704 (D.C. Cir. 1969); *see also* McClurg, *supra* note 86, at 991–92 (arguing that the intrusion tort should be expanded to give greater protection against surveillance conducted in public).

107 *Johnson*, 854 So. 2d at 549.

108 *See supra* Part I.A (discussing data collection practices).

109 *See* Richards & Solove, *supra* note 21, at 1919 ("Much of the compilation of data occurs from information that is in the public domain, and courts have concluded that collecting such data is not an invasion into a person's 'solitude' or 'seclusion.'"); Roethlisberger, *supra* note 19, at 1798 ("[Intrusion upon seclusion] is unlikely to be applied more broadly [to protect against the collection, use, and dissemination of personal information] because in most circumstances the user is giving up the information voluntarily.").

Busse v. Motorola, Inc. illustrates the difficulty of applying the intrusion tort to data collection.[110] The plaintiffs in the case brought suit against a private research firm that had obtained customer data from mobile service providers for use in a study investigating relationships between cell phone use and mortality.[111] The data included the customers' names, street addresses, dates of birth, Social Security numbers, and details regarding their wireless service accounts, including phone numbers, account numbers, and cell phone serial numbers.[112] This personal information was supplemented by data obtained from public death records and questionnaires mailed to customers that inquired into their cell phone usage habits.[113] At no point did the customers consent to or receive notice of the use of their personal information.[114]

The plaintiffs brought a class action against the research firm on behalf of customers whose information had been used in the study and included the intrusion tort among their claims.[115] In upholding the district court's grant of summary judgment against the plaintiffs, the *Busse* court stated that "none of the 'personal' information furnished by the customers, standing alone—names, telephone numbers, addresses or social security numbers—have been held to be private facts."[116] Consequently, the intrusion tort claim failed because there was no intrusion into a "private matter or private facts."[117]

Busse illustrates several reoccurring patterns in the case law. First, the *Busse* court based its holding on the secrecy paradigm and

---

110 813 N.E.2d 1013 (Ill. App. Ct. 2004).

111 *Id.* at 1015.

112 *Id.*

113 *Id.*

114 *Id.* at 1014–15.

115 *Id.* at 1013–15.

116 *Id.* at 1017. The court's pejorative use of scare quotes in the phrase "'personal' information" demonstrates a failure to distinguish between the concepts of private information and personal information. The information collected by the research firm was undoubtedly personal, as it described or identified the plaintiffs. *See supra* notes 59–62 and accompanying text (explaining a broad range of personal information). That the information may not have been private in no way diminishes the fact that it was personal.

117 *Busse*, 813 N.E.2d at 1017. The court's cavalier treatment of the disclosure of the customers' Social Security numbers may seem surprising given the confidentiality with which we generally regard such information. However, courts have consistently held that disclosure of Social Security numbers does not by itself support a claim of tortious intrusion, at least when the information had been voluntarily given to the disclosing party. *See* Johnson v. Stewart, 854 So. 2d 544, 549–50 (Ala. 2002) (establishing that the voluntary disclosure of Social Security numbers to defendant precludes intrusion tort claim based on defendant's subsequent provision of numbers to another party); Cooney v. Chicago Pub. Sch., 943 N.E.2d 23, 32 (Ill. App. Ct. 2010) (reaffirming *Busse* and holding that Social Security numbers do not constitute the type of "facially embarrassing and highly offensive" private facts protected by the intrusion tort).

the private-public dichotomy.[118] No tortious intrusion occurred because the research firm did not collect any data that the court considered to be private.[119] Second, the court viewed the case as involving only a single intrusion—the collection of data—and it assessed the privacy infringement from the intrusion by viewing the individual pieces of data collected "standing alone."[120] It did not consider how the aggregation of the consumer data with data from the death records and consumer questionnaires may uncover more intimate information and alter the privacy interests at stake.[121] The outcome of *Busse* may be appropriate even for an avid advocate of information privacy—it is not clear that possible links between an individual's cell phone usage and mortality fall under personal information[122]—but the *Busse* court's mechanical application of traditional tort doctrine hinders the adaption of the intrusion tort for combating modern privacy threats.

Dwyer v. American Express Co.[123] provides another example of the doctrinal obstacle posed by the secrecy paradigm. The *Dwyer* court held that credit cardholders' voluntary disclosures of their card usage histories to their credit card company precluded finding a tortious intrusion when the company compiled that information into consumer profiles and rented them out to other parties.[124] Because the cardholders had consented to divulge the data to the credit card company, further dissemination of that data by the company did not constitute an *unauthorized* intrusion.[125] Although the credit card company had aggregated the consumer records and created profiles of each cardholder based on their "behavioral characteristics and spending histories,"[126] the court did not consider the company's aggregation and analysis of the data as implicating a separate privacy intrusion.[127] Again, the intrusion tort proved wholly ineffective when applied to the intrusion occurring at the data collection stage.

---

118 *See Busse*, 813 N.E.2d at 1017–18 ("Because the analysis [of intrusion upon seclusion] begins with the predicate, private facts, it also ends there if no private facts are involved.").

119 *See id.* (noting the lack of "private facts" among the collected information).

120 *Id.* at 1017.

121 *See id.* at 1015 (discussing the research firm's methodology).

122 *See supra* notes 59–62 and accompanying text (defining what qualifies as personal information).

123 652 N.E.2d 1351 (Ill. App. Ct. 1995).

124 *Id.* at 1354.

125 *Id.*

126 *Id.* at 1353.

127 *See id.* at 1354 ("We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation.").

Commentators have argued that the secrecy paradigm has become outdated and should be discarded entirely.[128] Regardless of the merits of such contentions, courts are unlikely to completely reverse the secrecy paradigm, and "tort innovations can have a greater chance of adoption if they derive from established law."[129] The true obstacle posed by the secrecy paradigm flows from the application of the intrusion tort to the data collection stage of dataveillance. As Part III argues in greater detail, recognizing a distinct privacy intrusion in the information observation stage of dataveillance—in which "processed" personal information is extracted from the "unprocessed" data collected—can circumvent the secrecy paradigm.

B. Offensiveness of the Intrusion

The second doctrinal obstacle concerns the intrusion tort's offensiveness requirement. The intrusion tort requires an intrusion to be "highly offensive to a reasonable person" to be actionable.[130] Consequently, even if the intrusion concerned a private matter, it must still meet a high threshold of offensiveness. The offensiveness element is viewed as a "major obstacle" to applying the intrusion tort to data collection, as "[i]t is difficult [to] argue that simple collection of information freely given to a company would amount to something so 'highly offensive' to a reasonable person."[131] As Solove notes, "[e]ach particular instance of collection is often small and innocuous" and unlikely to reach the necessary degree of offensiveness.[132]

Busse v. Motorola, Inc. again is instructive.[133] Recall that *Busse* involved the collection of data from mobile service providers' customer records without the customers' consent.[134] In addition to holding that no tortious intrusion occurred because of the lack of privacy interest in the data collected, the *Busse* court noted that "the individual pieces of information—names, address[es], particulars of cell phone use—[are not] facially revealing, compromising or embar-

---

[128] *See* SOLOVE, *supra* note 11, at 143 (arguing that the secrecy paradigm is "outmoded in the Information Age" and should be abandoned).

[129] Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1810 (2010).

[130] RESTATEMENT (SECOND) OF TORTS § 652B (1977). Some courts discard the "highly" qualifier and require only that the intrusion be "offensive or objectionable to a reasonable man." *See, e.g.*, *Dwyer*, 652 N.E.2d at 1354 (citing Melvin v. Burling, 490 N.E.2d 1011, 1013–14 (Ill. App. Ct. 1986)) (adopting such a formulation). The precise difference between the two standards, if any, is unclear.

[131] Roethlisberger, *supra* note 19, at 1800.

[132] SOLOVE, *supra* note 11, at 59.

[133] 813 N.E.2d 1013 (Ill. App. Ct. 2004).

[134] *See supra* notes 111–17 and accompanying text (discussing facts of *Busse*).

rassing."[135] Because the *Busse* court considered only the intrusion from the data collection stage, it assessed the offensiveness of the intrusion by viewing each piece of data in isolation.[136] Although the court premised its holding on the lack of an intrusion into private facts or matters, the opinion's language indicates that the court would not consider the intrusion to be highly offensive even if the relevant information were private.[137] Other courts have dismissed intrusion claims involving the type of data likely to be collected for dataveillance,[138] including one's insurance history, unlisted telephone number, and magazine preferences.[139] Thus, in general, the intrusion at the data collection stage is unlikely to satisfy the offensiveness requirement.

However, as for the secrecy paradigm, the offensiveness requirement would not be a barrier to liability if courts recognize that dataveillance involves separate and distinct intrusions: one from the collection of data and subsequent intrusions from the observation of personal information. The offensiveness element could then be analyzed in light of the personal information observed during subsequent intrusions, which may be highly private and sensitive.[140] The next Part elaborates on this proposed doctrinal shift.

III
Recognizing Dataveillance's Privacy Intrusion at the Observation Stage

A. Dataveillance's True Privacy Invasion: Observation of Personal Information

As shown above, the two doctrinal obstacles of the secrecy paradigm and offensiveness requirement prevent the effective application of the intrusion tort to the data collection stage of dataveillance because the collected data are generally within the public domain and innocuous when viewed in isolation.[141] However, the benefit and

---

135 813 N.E.2d at 1018.

136 *See id.* (examining intrusiveness of privacy invasion in light of "individual pieces of information").

137 *See id.* (describing the information collected as not "revealing, compromising or embarrassing").

138 Solove, *supra* note 11, at 59.

139 *See* Tureen v. Equifax, Inc., 571 F.2d 411, 416 (8th Cir. 1978) (dismissing a privacy claim for collection of insurance history); Seaphus v. Lilly, 691 F. Supp. 127, 132 (N.D. Ill. 1988) (dismissing a privacy claim for obtaining an unlisted telephone number); Shibley v. Time, Inc., 341 N.E.2d 337, 339–40 (Ohio Ct. App. 1975) (dismissing a privacy claim for selling magazine subscription lists).

140 *See supra* Part I.A (discussing Big Data's capability of uncovering hidden personal information).

141 *See supra* Part II (describing doctrinal obstacles).

danger of dataveillance lay in the extraction of hidden facts and patterns about individuals from the processing of those pieces of data. Through aggregation and mining, dataveillance allows observation of "processed" information that is much more revealing than the sum of the "unprocessed" data, as data that "appears innocuous can sometimes be the missing link, the critical detail in one's digital biography, or the key necessary to unlock other stores of personal information."[142] Thus, dataveillance's true privacy threat occurs at the information observation stage.

Consequently, the intrusion tort should recognize that dataveillance's observation of new personal information, unknown and unknowable from the individual pieces of data, constitutes a separate privacy intrusion, distinct from the intrusion occurring at the data collection stage. This recognition would allow the doctrinal elements of the tort to be assessed in light of the subsequent intrusion at the observation stage. Such observation will not always constitute a tortious intrusion—it must still satisfy each of the tort's elements—but recognizing that dataveillance's observation stage effects a distinct privacy intrusion helps overcome the doctrinal obstacles of the secrecy paradigm and offensiveness requirement.[143]

The normative justification for holding the observation of personal information to be a distinct privacy intrusion is simple. As explained above, the protection of information privacy promotes important values.[144] Granting individuals control over personal information about themselves helps protect interests such as "dignity, autonomy, and self-determinism."[145] The unwanted observation of one's personal information constitutes an invasion of privacy, whether it occurs through traditional methods of surveillance or through the modern method of dataveillance. The more difficult question is whether the proposed framework—one in which dataveillance's observation stage itself may constitute a tortious invasion of privacy—is tenable as a matter of doctrine. This Note argues that the answer is yes.

Prosser's canonical formulation of the intrusion tort firmly recognizes that it applies to nonphysical invasions of privacy, such as sur-

---

[142] SOLOVE, *supra* note 11, at 44; *see also* Solove, *supra* note 18, at 507 ("A piece of information here or there is not very telling. But when combined together, bits and pieces of data begin to form a portrait of a person. The whole becomes greater than the parts.").

[143] *See infra* Parts III.B–C (discussing doctrinal implications of the proposed shift).

[144] *See supra* notes 63–65 and accompanying text (discussing normative values of information privacy).

[145] Bambauer, *supra* note 31, at 213.

reptitious surveillance.[146] Prosser noted that the intrusion tort had been applied to "eavesdropping upon private conversations" through the use of wiretapping and microphones and to "peering into the windows of a home."[147] More recently, courts have allowed intrusion claims based on the interception of private phone calls,[148] secret videotaping of private matters,[149] unauthorized inspection of personal credit history,[150] and unconsented examination of credit card records, even when the records were lawfully within the defendant's possession.[151] The viability of intrusion upon seclusion in those cases demonstrates that the intrusion tort can apply to surveillances even absent some trespass-related misconduct and even if the victim is initially unaware of the surveillance.

Most on point, the intrusion tort protects against nonconsensual testing of blood and urine samples, even if the samples themselves were procured legally. Courts have recognized that "the act of extracting a blood sample and the tests performed upon the sample are *separate intrusions*," necessitating the application of the intrusion tort's elements to each intrusion.[152] Because individuals maintain a privacy interest in the medical information that may be gleaned from

---

[146] *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977) (stating that liability for tortious intrusion may attach to "[o]ne who intentionally intrudes, physically *or otherwise*" (emphasis added)); *id.* cmt. b (stating that tort protects against invasions of privacy "by the use of the defendant's senses" or "by some other form of investigation or examination into [the plaintiff's] private concerns"); Prosser, *supra* note 78, at 390 ("The principle [of intrusion upon seclusion] was . . . soon carried beyond . . . physical intrusion.").

[147] Prosser, *supra* note 78, at 390.

[148] *See* Luken v. Edwards, No. C10–4097–MWB, 2011 WL 1655902, at *5 (N.D. Iowa May 3, 2011) (allowing an intrusion claim based on the interception of telephone calls between plaintiff and her lawyer during divorce proceeding).

[149] *See* Webb v. CBS Broad. Inc., No. 08 C 6241, 2009 WL 1285836, at *3 (N.D. Ill. May 7, 2009) (emphasizing that the act of secretly videotaping into plaintiff's backyard from a neighbor's home itself can constitute an intrusion upon seclusion, regardless of the publication of the videotape); Baugh v. Fleming, No. 03-08-00321-CV, 2009 WL 5149928, at *2 (Tex. App. Dec. 31, 2009) (allowing a claim based on "videotaping through the window of a home" despite the absence of a physical intrusion).

[150] *See* Hall v. Harleysville Ins. Co., 869 F. Supp. 478, 484 (E.D. Pa. 1995) (holding that a question of fact existed as to whether an unauthorized search of credit history could constitute an intrusion upon seclusion).

[151] *See* Pulla v. Amoco Oil Co., 882 F. Supp. 836, 866–67, 867 n.24 (S.D. Iowa 1994) (allowing intrusion claim based on employer's examination of employee's credit card records, even though employer lawfully held records in employment files).

[152] Doe v. High-Tech Inst., Inc., 972 P.2d 1060, 1069 (Colo. App. 1998) (emphasis added); *see also* Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260, 1268–70 (9th Cir. 1998) (giving blood and urine samples to an employer consensually does not necessarily constitute consent for the testing of the samples for various diseases and does not bar a claim under federal and state constitutional rights to privacy); Havasupai Tribe of the Havasupai Reservation v. Ariz. Bd. of Regents, 204 P.3d 1063, 1076 (Ariz. Ct. App. 2008) (citing *High-Tech Institute* and *Norman-Bloodsaw* approvingly in a case involving unauthorized testing of blood samples).

their bodily fluids, an unauthorized test can establish a claim under the intrusion tort, even if the fluids were relinquished voluntarily.[153] The objectionable intrusion "is not the physical test of a [fluid] sample itself," but rather the unwanted observation of "highly personal medical information [that] may be obtained from such test."[154] The unauthorized testing in these cases resembles dataveillance in that both involve the unauthorized observation of "processed" information extracted from an "unprocessed" source that may have been collected lawfully. Thus, it would not be a doctrinal leap to apply the intrusion tort to dataveillance's observation stage. Indeed, focusing on the observation aspect of nonphysical intrusions may better encapsulate the true interest that the tort seeks to protect when applied to nonphysical intrusions, that of information privacy.[155]

Other fields of the law concerning privacy also provide support for this Note's proposal. In *United States Department of Justice v. Reporters Committee for Freedom of the Press*,[156] the Supreme Court determined that the Freedom of Information Act (FOIA) does not require disclosure of an individual's FBI "rap sheet," because the statute exempted law enforcement records that may result in an unwarranted privacy invasion if released.[157] The party seeking disclosure contended that only a minimal privacy interest existed in a rap sheet because it merely summarized information about an individual's criminal record, much or all of which has been previously disclosed in various public documents.[158] The Court disagreed, noting the "vast difference" between scattered disclosures of bits of information in hard-to-obtain public records and a central clearinghouse containing all relevant information.[159] Thus, *Reporters Committee* supports the principle that aggregation of data, even if collected from public sources, can alter and compound the underlying privacy interest when the aggregated whole is more revealing than the sum of its parts.[160]

Further support may be drawn from cases interpreting the Fourth Amendment's stricture against unreasonable searches that violate an

---

153 *High-Tech Inst.*, 972 P.2d at 1068.

154 *Id.* at 1069–70.

155 *See* Bambauer, *supra* note 31, at 238 ("[I]t is *observation* . . . that is at the heart of an intrusion.").

156 489 U.S. 749 (1989).

157 *Id.* at 779.

158 *Id.* at 760, 762–63.

159 *Id.* at 764.

160 *See id.* (endorsing the distinction between "scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole"); Solove, *supra* note 18, at 509–10 (noting that *Reporters Committee* recognizes that aggregation of data may violate privacy if it "significantly increases what others know about a person, even if originating from public sources").

individual's reasonable expectation of privacy.[161] Like the intrusion tort, the Fourth Amendment follows the secrecy paradigm and generally does not protect activities in the public sphere.[162] However, several courts have endorsed the view that pervasive government surveillance of nonprivate conduct may still violate a reasonable expectation of privacy if the entirety of the information collected by the government provides a much more revealing picture than any single piece of information viewed in isolation. In *United States v. Maynard*, the D.C. Circuit Court of Appeals held that constant Global Positioning System (GPS) tracking of the defendant's automobile over one month infringed upon a reasonable expectation of privacy, even though each movement of the automobile was exposed to the public.[163] Invoking *Reporters Committee*'s recognition of the transformative effect of aggregation, the court noted the qualitative difference between disclosing isolated movements to the public and having the entirety of one's movements tracked.[164] Pervasive GPS surveillance records the frequencies and sequences of an individual's movements, which can "reveal more about a person than does any individual trip viewed in isolation."[165] For example, "a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story."[166] Thus, *Maynard* implicitly recognizes that an individual may

---

[161] The Fourth Amendment prohibits the State from conducting unreasonable and warrantless searches and seizures. Under the modern view, first developed in Justice Harlan's concurrence in *Katz v. United States*, a search occurs when the State intrudes upon an individual's reasonable expectation of privacy. 389 U.S. 347, 361–62 (1967) (Harlan, J., concurring). To establish a reasonable expectation of privacy, an individual must exhibit a subjective expectation of privacy, which society recognizes as reasonable. *Id.* at 361. Although the Fourth Amendment constrains government and not private actors, courts have borrowed from Fourth Amendment principles in applying the intrusion tort. *See, e.g.*, Pearson v. Dodd, 410 F.2d 701, 704 (D.C. Cir. 1969) ("Just as the Fourth Amendment has expanded to protect citizens from government intrusions where intrusion is not reasonably expected, so should tort law protect citizens from other citizens.").

[162] *See* United States v. Knotts, 460 U.S. 276, 281–82 (1983) (holding that individuals have no reasonable expectation of privacy in movements made in public); Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

[163] 615 F.3d 544, 558 (D.C. Cir. 2010), *aff'd on other grounds sub nom*. United States v. Jones, 132 S. Ct. 945 (2012).

[164] *Id.* at 561–62. In so doing, the court distinguished the case from *United States v. Knotts*, in which the Supreme Court held that use of an electronic beeper to track the defendant's public movements over a short distance did not implicate a cognizable privacy interest because the defendant lacked a reasonable expectation of privacy in such movements. 460 U.S. at 282.

[165] *Maynard*, 615 F.3d at 562.

[166] *Id.*

have a privacy interest in the inferences and new information that may be drawn from a collection of data, even if each piece of data had been disclosed to the public.[167]

In *Klayman v. Obama*, a federal district court applied a similar principle, finding that the National Security Agency (NSA) likely violated the Fourth Amendment in systematically collecting and analyzing American citizens' phone record "metadata,"[168] including "information about what phone numbers were used to make and receive calls, when the calls took place, and how long the calls lasted."[169] Though the metadata records did not disclose the content of or parties to any phone calls, the NSA applied advanced computerized searches to vast amounts of data to identify connections between foreign terrorist organizations and domestic terrorist operatives.[170] In other words, the NSA conducted a program of dataveillance that aggregated and mined data to uncover hidden patterns and information. The court rejected the government's position that no expectation of privacy existed in the metadata because the information contained within it was voluntarily disclosed to users' telecommunication service providers, instead finding that the NSA program constituted a search, implicating a reasonable expectation of privacy under the Fourth Amendment.[171] Noting the "almost-Orwellian technology"[172] used by

---

[167] *Maynard* reached the Supreme Court as *United States v. Jones*, 132 S. Ct. 945 (2012). The Court unanimously held that the government conducted a search under the Fourth Amendment but fractured in its reasoning. *Id.* at 945, 949. The majority opinion wholly ignored whether the tracking implicated a reasonable expectation of privacy and instead held that the government's physical trespass in attaching the GPS device to defendant's car sufficed to constitute a search. *Id.* at 949. Four concurring Justices criticized the majority's approach, *id.* at 958–61 (Alito, J., concurring), and concluded, without much elaboration, that the long-term GPS tracking did in fact violate a reasonable expectation of privacy. *Id.* at 964. Justice Sotomayor, while joining the majority opinion, wrote a separate concurrence voicing concerns regarding the transformative power of dataveillance. Noting that "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse," Justice Sotomayor questioned "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." *Id.* at 956 (Sotomayor, J., concurring). Thus, while *Jones* did not explicitly adopt the approach in *Maynard*, at least five justices (the three joining the Alito concurrence and Justice Sotomayor) can be viewed as approving the Court of Appeals' reasoning.

[168] *See* Klayman v. Obama, 957 F. Supp. 2d 1, 9–10 (D.D.C. 2013), *cert. denied*, 134 S. Ct. 1795 (2014) (stating that the plaintiffs "have demonstrated a substantial likelihood of success on the merits of their Fourth Amendment claim").

[169] *Id.* at 14.

[170] *See id.* at 15–18 (describing the operation of the NSA's surveillance program).

[171] *See id.* at 30–31 (distinguishing *Klayman* from previous Supreme Court precedent).

[172] *See id.* at 33 ("It's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our

the NSA in mining metadata for information,[173] the court emphasized that such dataveillance can "reveal an entire mosaic—a vibrant and constantly updating picture of the person's life."[174] Thus, *Klayman* supports the principle that the aggregation and mining of metadata may result in a privacy intrusion distinct from the initial collection of the records themselves.[175]

B. Overcoming the Doctrinal Obstacles

As demonstrated above, viewing dataveillance's observation of new personal information as constituting a separate privacy intrusion is doctrinally consistent with existing applications of the intrusion tort. It also draws support from principles recognized in the context of FOIA and the Fourth Amendment. This Subpart elaborates on how the proposed doctrinal shift helps overcome the twin hurdles of the secrecy paradigm and offensiveness requirement without making every use of dataveillance per se tortious. The intrusion tort's doc-

---

citizens expect all phone companies to operate what is effectively a joint intelligence-gathering operation with the Government.").

[173] *See id.* ("[T]he Government has at its disposal today the most advanced twenty-first century tools, allowing it to 'store such records and efficiently mine them for information years into the future.'" (quoting United States v. Jones 132 S. Ct. 945, 956 (Sotomayor, J., concurring)).

[174] *Id.* at 36 (citing United States v. Maynard, 615 F.3d 544, 562–63 (2010)). The *Klayman* court rejected the government's contention that the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979), controlled the outcome of the case. *Id.* at 30–31. The Court in *Smith* affirmed the warrantless installation of a pen register that recorded the telephone numbers dialed from an individual's phone, 442 U.S. at 745–46, holding that individuals lack reasonable expectations of privacy in the numbers they dial, because they necessarily disclose such information to their telephone companies. *See id.* at 742–44 (distinguishing between the content of phone conversations conducted between two persons and the phone numbers individuals communicate to third parties). The *Klayman* court characterized the situation in *Smith* as "a far cry from the issue in this case." *Klayman*, 957 F. Supp. 2d at 31. Instead, the *Klayman* court held *Smith* to be wholly inapplicable, noting that the NSA conducted a much more prolonged, pervasive, and technologically advanced surveillance program than that in *Smith*, while highlighting the more integral role that cellphones occupy in modern life compared to telephones three decades ago. *See id.* at 32–36 ("[T]he Court in 1979 [never could have] imagined how the citizens of 2013 would interact with their phones.").

[175] The saga of the NSA's dataveillance program remains ongoing. The Supreme Court denied the government's interlocutory appeal from *Klayman*'s grant of a preliminary injunction. Klayman v. Obama, 134 S. Ct. 1795 (2014). Meanwhile, another federal district court upheld the constitutionality of the program in a separate case. ACLU v. Clapper, 959 F. Supp. 2d 724, 730 (S.D.N.Y. 2013). Unlike the court in *Klayman*, the *Clapper* court accepted the argument that *Smith* controlled the issue. *See id.* at 752 (arguing that the Supreme Court has never overturned *Smith*, and that the NSA program is similar to the collection of data through pen register); *see also supra* note 174 (discussing *Klayman* court's rejection of the applicability of *Smith*). Regardless of the ultimate outcome, the *Klayman* court's reasoning remains sound. *See supra* Part III.A (discussing the tortious impact of privacy invasions caused by metadata observation).

trinal elements would continue to circumscribe liable conduct, but they would not bar the application of the tort.

1. Overcoming the Secrecy Paradigm

The proposed doctrinal shift would circumvent the secrecy paradigm without needing to overturn it altogether. Recall that the secrecy paradigm views individuals as lacking a substantial privacy interest in data that has been disclosed or placed in the public domain.[176] Recognition that the intrusion tort protects against the unwanted observation of personal *information* and not just against the initial collection of *data* maintains the viability of the intrusion tort, even when the data collected was previously divulged to third parties or made available in public records. Disentangling the privacy interest in observed information from the privacy interest in collected data shifts the relevant assessment to whether that information was kept private from the observer, rather than whether secrecy had been maintained in the data. Under this doctrinal shift, if dataveillance results in observation of personal information that was never voluntarily disclosed, that information is private, not public, even if the raw data used to obtain that information was in the public domain.

The problem remains of defining when dataveillance results in a sufficient observation of new personal information to constitute a distinct privacy intrusion. Jane Yakowitz Bambauer proposes a definition based on the purpose for which the data was collected relative to the manner in which it was used, with a potentially tortious observation occurring when "personal data is used or disclosed for some purpose *inconsistent* with its original collection without advance notice and consent."[177] While this approach serves the laudatory function of recognizing that "individuals want to keep things private from some people but not others,"[178] it does not fully capture the interests protected by information privacy. Information privacy is about individual control over personal information,[179] and a purpose-based test does not necessarily measure whether an observation of personal information has occurred. Consistent use of data may result in the observation of new personal information—for example, the analysis of credit card records to create consumer profiles in *Dwyer*.[180] At the same time,

176 *See supra* Part II.A (discussing the secrecy paradigm).

177 Bambauer, *supra* note 31, at 252 (emphasis added).

178 *See* SOLOVE, *supra* note 11, at 43–44 (arguing privacy means personal information will not be used to circumvent the wishes of an individual, and that individuals may expect privacy even when in public).

179 *See supra* Part I.B (explaining the interest of information privacy).

180 *See supra* notes 123–27 and accompanying text (discussing *Dwyer*).

inconsistent data use may not lead to that same observation, as highlighted in *Busse*.[181]

This Note proposes a definition of observation that matches the broad range of personal information protected by information privacy: Dataveillance causes a potentially tortious observation when the aggregation and mining of data results in meaningful recognition of personal information that is substantially different from information recognizable from individual pieces of raw data. Thus, for the purpose of the intrusion tort, an observation occurs when dataveillance uncovers "processed" information that is substantially more revealing than the sum of the "unprocessed" data. If such observation was the intended effect of dataveillance, then an intentional intrusion has occurred. While this definition offers an expansive view of what may be considered an intrusion, the range of *tortious* intrusions remains limited by the elements of the tort, as described below.

2. *Overcoming the Offensiveness Requirement*

Recognition that dataveillance's observation stage constitutes a distinct privacy intrusion also affects analysis of the intrusion tort's offensiveness requirement. Dataveillance's data collection stage, involving previously disclosed and relatively innocuous pieces of data, is unlikely to be so "highly offensive" as to become a tortious intrusion.[182] If the subsequent observation of information itself qualifies as an intrusion, however, then the degree of offensiveness should be assessed in the context of that observation.

While the offensiveness element of the intrusion tort ultimately depends on fact finders' case-by-case determinations,[183] it may be useful to delineate more precisely how the offensiveness of a dataveillance observation should be assessed. Given that an unwanted observation of personal information infringes on the interest of information privacy, it follows that its offensiveness depends on the degree to which the observation subverts an individual's control over the "acquisition, disclosure, and use" of that personal information.[184] As Solove explains, "people selectively spread around small pieces of

---

[181] *See supra* notes 110–21 and accompanying text (discussing *Busse*).

[182] *See supra* Part II.B (discussing the offensiveness requirement).

[183] *See, e.g.*, Pulla v. Amoco Oil Co., 882 F. Supp. 836, 867 (S.D. Iowa 1994) (finding that a reasonable jury could have found defendant's privacy intrusion to be highly offensive to a reasonable person in light of facts presented).

[184] *See* Kang, *supra* note 17, at 1203 (discussing privacy concerns related to the transmission of personal information). This understanding suggests that Bambauer's purpose-based test for defining when an observation occurs—evaluating if personal data was used or disclosed for a purpose inconsistent with its original collection—can more appropriately fit the offensiveness prong of the intrusion tort. *See* Bambauer, *supra* note

data . . . and they have the expectation that in each disclosure, they are revealing relatively little about themselves."[185] By aggregating data and extracting from them personal information that is unrelated to the purpose consumers expect that data to serve, dataveillance "unsettles expectations" regarding what individuals actually consented to reveal in disclosing the individual pieces of data.[186]

Thus, offensiveness should be judged by comparing the nature of the new information observed through dataveillance with the nature of the information that an individual reasonably expected would be revealed when disclosing that data.[187] The greater the dissonance between the type of information *actually* observed and the type of information *expected* to be disclosed, the more severely privacy expectations become unsettled, and the more likely a reasonable person would find that observation "highly offensive." The observation of highly sensitive personal information through the use of apparently innocuous data is likely to seriously disturb privacy expectations, although, strictly speaking, the sensitivity and confidentiality of the observed information are not, by themselves, dispositive factors under this test for offensiveness. Though flipping the traditional analysis on its head, this objective inquiry resembles the "harm within the risk" theory of proximate causation, which holds a defendant responsible for injuries falling within the scope of the risk created by their negligent conduct.[188] Here, no liability attaches if dataveillance observes information "within the risk" of expected disclosures at the time of data collection, while an observation may be highly offensive if dataveillance uncovers information outside of the scope of the risk.

Admittedly, this framework proposes a standard rather than a bright-line rule for determining when an observation meets the offensiveness requirement. It relies on a comparison of what information

---

31, at 252 (proposing a purpose-based framework for determining occurrence of observation).

185 *See* Solove, *supra* note 18, at 508 (discussing the dignitary harms that data aggregation can cause).

186 *See id.* ("People expect certain limits on what is known about them and on what others will find out.").

187 This formulation comports with Bambauer's assessment of an observation's offensiveness. *See* Bambauer, *supra* note 31, at 245 ("The offensiveness element winds up turning on whether the observed could have and should have expected their information to be exposed to the observer."). However, it refines Bambauer's approach by elucidating exactly what makes the observation offensive: the disturbance of individuals' privacy expectations.

188 *See* ROBERT E. KEETON, LEGAL CAUSE IN THE LAW OF TORTS 9 (1963) (noting that liable negligence requires the harm to "result within the scope of at least one of the risks on the basis of which the actor is found to be negligent"); Richard W. Wright, *Causation in Tort Law*, 73 CALIF. L. REV. 1735, 1763–64 (1985) (critiquing the "harm within the risk" theory of causation).

an individual reasonably expected to be revealed from disclosed data with what information the data actually revealed when aggregated and mined. But the offensiveness of any privacy intrusion turns on such contextual judgments.[189] "[Privacy law] is the product of local social anxieties and local ideals,"[190] and the proposed standard allows fact finders to determine "what sorts of seclusion we instinctively expect to have" in the modern world and when dataveillance violates those expectations.[191]

C. Applying the Proposed Doctrinal Shift

This Subpart applies this Note's proposals to some examples, demonstrating their functionality. The three instances reviewed are Target's "pregnancy-prediction model," the use of cell phone users' customer data in a research study in *Busse*, and the compilation of credit card purchase data into consumer profiles in *Dwyer*.

Target's use of customers' purchase records to discover pregnancy information presents the most likely instance of a tortious intrusion through observation of processed data. Recall that the company used receipts for items such as cotton balls and hand lotions to determine with substantial certainty the pregnancy statuses and due dates of its customers.[192] The intrusion tort would provide no remedy if applied to the data collection stage, since data from each purchase was voluntarily disclosed and inoffensive when viewed in isolation.

However, viewing Target's observation of its customers' pregnancy statuses as a separate privacy intrusion may alter the outcome. A woman's pregnancy status constitutes personal information over which she should retain control. Such information is not recognizable from the unprocessed data disclosed during each purchase. Thus, the observation of pregnancy presents a distinct privacy intrusion. Is the observation sufficiently offensive to constitute a tortious intrusion? Although the answer ultimately rests on a subjective, contextual assessment, the disparity between the type of information reasonably expected to be disclosed from each purchase (a purchase of a product at a certain time in a certain store) and the actual information being

---

[189] *See, e.g.*, Pulla v. Amoco Oil Co., 882 F. Supp. 836, 867 (S.D. Iowa 1994) (finding that a reasonable jury could have found the defendant's privacy intrusion to be highly offensive to a reasonable person in light of the facts presented).

[190] *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1219 (2004) (arguing that the concept of privacy is not the product of "logic," "experience," or "supposed felt necessities").

[191] *See* Bambauer, *supra* note 31, at 248 (discussing judges' and juries' basis for understanding the Internet).

[192] *See supra* notes 1–7 and accompanying text (discussing Target's dataveillance methods).

observed (pregnancy status and due date) certainly could be "highly offensive to a reasonable person."[193] Application of the intrusion tort to the observation stage rather than the data collection stage thus provides a safeguard against Target's overly intrusive dataveillance.

The facts of *Busse*, involving the collection of cell phone users' data for a study examining potential links between cell phone usage and mortality, demonstrates that the proposed doctrinal shift does not create liability for every collection and use of data. The *Busse* court assessed the elements of the intrusion tort in light of the individual pieces of data collected, finding that no tortious intrusion occurred because none of the data involved private facts or matters.[194] Applying the intrusion tort to the observation of information extracted from the data should result in the same outcome. Specifically, the information that the research study attempted to uncover—causal links between cell phone usage and mortality—should not be considered *personal* information, as it is not "information identifiable to the individual."[195] Thus, the study neither constituted observation of personal information or a privacy intrusion.

Finally, the facts of *Dwyer* demonstrate how the offensiveness requirement can still have a limiting effect when applied to the observation stage of dataveillance. *Dwyer* involved a credit card company aggregating customers' credit card usage data to create revealing consumer profiles that were then rented out to other parties.[196] The court found no unauthorized privacy intrusion, because each piece of data was voluntarily disclosed to the credit card company.[197] However, the aggregation and analysis of the data revealed cardholders' spending habits and shopping preferences, which comprises personal information unrecognizable from the individual pieces of data viewed in isolation.[198] Thus, the observation of that personal information results in a distinct and unauthorized privacy intrusion.

---

[193] *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977) (providing elements of the intrusion upon seclusion tort).

[194] *See* Busse v. Motorola, Inc., 813 N.E.2d 1013, 1017 (Ill. App. Ct. 2004) (holding that the defendants did not publicly disclose "private facts" related to the plaintiffs and rendering the plaintiffs without a cause of action).

[195] *See* Kang, *supra* note 17, at 1206 (citation omitted) (describing personal information as a central component of "nearly all definitions of information privacy").

[196] Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1353 (Ill. App. Ct. 1995).

[197] *Id.* at 1354 ("We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation.").

[198] *See* Karas, *supra* note 33, at 397–98 (arguing that "a recognizable portrait of us materializes" when seemingly isolated personal records are collected, and that the "examination of consumer records produces a fairly accurate psychological profile").

The inquiry still requires ascertaining the offensiveness of the intrusion by comparing the nature of the information expected to be revealed from disclosed data with the nature of information actually observed. Here, the two variables exhibit a close relationship. Each credit card purchase reveals something about the cardholder's commercial preferences. While a comprehensive consumer profile provides a more telling picture, the discrepancy between the information expected to be revealed (commercial preferences) and the information actually observed (a comprehensive consumer profile) does not seem so severe as to greatly unsettle the cardholder's reasonable privacy expectations.[199] Thus, while the dataveillance resulted in a secondary privacy intrusion, that intrusion is unlikely to be "highly offensive to a reasonable person."[200]

D. Assessing Potential Counterarguments

Applying the intrusion tort to dataveillance's information observation stage rather than its data collection stage alleviates the doctrinal obstacles of the secrecy paradigm and the offensiveness requirement without creating an outcome determinative regime that makes every instance of dataveillance a tortious intrusion. In this way, the tort of intrusion upon seclusion could be adapted to provide some protection against the privacy threats of the modern world. However, such an approach presents potential drawbacks as well. This Subpart examines some counterarguments against this Note's proposal.[201]

An initial objection may be that the intrusion tort does not provide sufficient ex ante predictability for determining when dataveillance would constitute a tortious privacy intrusion. The tort's reliance on a context-sensitive standard necessarily increases the unpredict-

---

[199] To be sure, a distinction exists between the basic transactional facts surrounding each credit card transaction and the commercial preferences that may be inferred from those facts. A consumer consenting to disclose the transactional facts nevertheless may not desire to reveal his or her commercial preferences to the credit card company. Still, the transactional facts—when, where, and why a customer used his or her credit card—inevitably and directly say something about the underlying preference motivating that transaction. Therefore, the consumer should reasonably expect to disclose some information regarding commercial preferences in disclosing the transactional data. Consequently, compiling transaction data to form a consumer profile should not so severely disturb the consumer's privacy expectations to constitute a highly offensive privacy intrusion.

[200] RESTATEMENT (SECOND) OF TORTS § 652B (1977); *see also* Bambauer, *supra* note 31, at 246–47 (viewing the observation of transaction data as unlikely to meet the offensiveness requirement).

[201] This Subpart does not address all relevant concerns. Some issues are beyond the scope of this Note, such as the assessment of monetary damages for privacy harms and the First Amendment implications of regulating dataveillance.

ability of legal outcomes, which may over-deter socially beneficial conduct.[202] Such concerns are overstated, however. Companies engaging in dataveillance understand what data will be used and what personal information may be uncovered. Thus, they are well-placed to predict the unsettlement of privacy expectations that may result from each particular use of dataveillance. Moreover, at least in some instances, companies can shape privacy expectations at the front-end through the use of notices at the data collection stage. While pro forma notice and consent do not adequately protect privacy rights,[203] the presence of genuine notice that the data collected may be used to uncover other personal information would be relevant to determining whether dataveillance sufficiently disrupted privacy expectations to constitute a tortious privacy intrusion. Thus, companies can reasonably predict and control their potential liability.

A thornier problem is that dataveillance observations of personal information are often predictive rather than conclusive.[204] For example, even Target's "pregnancy-prediction model," which could predict pregnancy status with a high degree of accuracy,[205] falls short of certainty. Must a dataveillance practice be one hundred percent accurate to cause tortious intrusions? Doctrinally, the answer should be no. The intrusion tort applies to unconsented testing of blood and urine samples,[206] which does not uncover medical information with complete accuracy and thus also involves probabilistic observations. However, the issue remains of determining whether some accuracy threshold limits the range of potentially tortious observations. This Note does not attempt to definitively resolve this concern, which implicates complex questions of what it means to observe information or to know a fact. One potential solution would be to ignore altogether the accuracy of a dataveillance method at the macro scale and focus instead on the individual's loss of privacy at the micro scale. Under this approach, dataveillance results in a potentially tortious privacy intrusion if it intends to observe a type of personal information

---

[202] *See supra* notes 189–91 and accompanying text (explaining that the intrusion tort necessitates a certain degree of subjectivity).

[203] *See, e.g.*, Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1186 (2011) (summarizing the common criticisms of consent as an effective form of privacy protection).

[204] *See* Ian Kerr & Jessica Earle, *Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy*, 66 STAN. L. REV. ONLINE, 65, 66–67 (2013), http://www.stanfordlawreview.org/online/privacy-and-big-data/prediction-preemption-presumption (describing Big Data's predictive capabilities).

[205] Duhigg, *supra* note 1, at 37.

[206] *See, e.g.*, *supra* notes 152–55 and accompanying text (detailing Doe v. High-Tech Inst., Inc., 972 P.2d 1060 (Colo. App. 1998), as such an example).

about an individual, makes a predictive observation regarding that information, and that prediction turns out to be accurate. The expected accuracy of the observation would not matter so long as the privacy harm did in fact occur.

Finally, one might fundamentally question tort law's ability to appropriately balance the costs and benefits associated with dataveillance. Courts and juries are not as well-situated as legislators to make such policy determinations, and imposing tort liability might overdeter the societal benefits provided by the multibillion-dollar dataveillance industry.[207] However, the current legal regime lacks any comprehensive check against abusive dataveillance practices.[208] While tort law may not be the optimal method of regulation, it can provide a stopgap solution until a legislative or regulatory response emerges. As Bambauer argues, one of tort law's objectives is to achieve the proper level of deterrence against socially harmful behavior, and a tort-based approach may work well to balance the risks and utilities of dataveillance.[209] Thus, this Note's proposal limits liability to unwanted observations that seriously disturb reasonable privacy expectations, since such a framework deters only conduct infringing upon privacy without unduly affecting the entire dataveillance industry.

Conclusion

"The story of privacy law is a tale of changing technology and the law's struggle to respond in effective ways."[210] Warren and Brandeis developed the concept of a right to privacy in response to the technological innovations of their time.[211] The modern era has brought about new technological advances and new privacy threats, requiring the common law to evolve accordingly. The overly intrusive use of dataveillance—a practice that remains largely unregulated—is one of the twenty-first century's challenges to privacy. This Note's proposal would update the traditional tort of intrusion upon seclusion to operate as an effective check against the modern privacy threat of dataveillance.

---

[207] *See* Singer, *supra* note 33, at BU8 (discussing the industry of large-scale data mining and analytics).

[208] *See supra* notes 74–75 and accompanying text (discussing gaps in privacy law).

[209] *See* Bambauer, *supra* note 31, at 227–28 ("[A]n optimal collection of privacy regulations will deter the sorts of information flows that tend to create more disutility than utility. This is exactly what common law tort rules aspire to do.").

[210] *See* Solove, *supra* note 11, at 56 (discussing various forms of law comprising information privacy law and arguing that there is not yet a "compelling theory of privacy").

[211] *See supra* notes 77–82 and accompanying text (discussing Warren and Brandeis's seminal law review article).