Articles

Privacy Harms

IGNACIO N. COFONE* & ADRIANA Z. ROBERTSON**

Privacy loss is central to privacy law scholarship, but a clear definition of the concept remains elusive. We present a model that both captures the essence of privacy loss and can be easily applied to policy evaluations and doctrinal debates. To do so, we use standard Bayesian statistics to formalize a key intuition: that information privacy is fundamentally linked to how much other people know about you. A key advantage of our model is that, for the first time, it takes privacy preferences seriously while maintaining tractability. Another key advantage is that, by viewing privacy as a continuum, it is more realistic and is better suited for evaluating "gray areas" than prior models.

We apply this framework to two central areas of privacy law: the common law privacy tort and the Fourth Amendment's third party doctrine. In the tort context, we first show how our proposal helps to clarify current law, and then use it to distinguish between the two interests protected by the privacy tort: privacy interests and reputational interests. We then propose a simple framework for judges to use in providing remedies for both classes of claims. We then move on to the third party doctrine. We show that many of the shortcomings associated with the doctrine stem from the misguided assumption that privacy is dichotomous rather than a spectrum, as in our model. We then liken this to the standard of care familiar from tort law, and show how the current doctrine results in the equivalent of a strict liability standard, rather than a more appropriate negligence-based standard.

[*] Post-doctoral research fellow, NYU Information Law Institute.

[**] Assistant Professor, University of Toronto Faculty of Law and Rotman School of Management. The Authors would like to thank Abi Adams, BJ Ard, Ian Ayres, Jack Balkin, Thomas Bonczek, Kiel Brennan-Marquez, Justin Brookman, Rebecca Crootof, Joshua Fairfield, Claudia Haupt, Christine Jolls, Thomas Kadri, Michael Klausner, M. Henry Linder, Asaf Lubin, Clara Marsan, Helen Nissenbaum, Katherine Strandburg, Eduardo Stordeur, and Ari Waldman for their helpful suggestions. We also thank two referees, as well as Jacob Hirsch, Christa Hall, and the editorial staff of the *Hastings Law Journal*. This Article benefited from discussions with participants at the Internet Law Works-in-Progress Symposium, the Privacy Law Scholars Conference Europe, and an internal presentation at Yale Law School.

TABLE OF CONTENTS

INTRODUCTION

Most people care about their privacy. For example, less than three months into the year, a Google news search for "privacy 2018" returned 131,000,000 results.[1] Yet despite the importance of information privacy in modern society, privacy harms are hard to pin down. This, in turn, creates challenges for information privacy law, since a clear conception of these harms is essential for determining both standing and remedies. As a leading information privacy law casebook put it: "an overarching issue in privacy cases is whether the privacy violation caused any harm . . . in both data security breach cases and privacy cases, courts have struggled to recognize [such] harm."[2] Unfortunately, information privacy is hard to pin down.

Scholars have approached privacy in two different ways.[3] Drawing on insights from economics, philosophy and sociology, the first approach focuses on the normative value of privacy, and tries to answer the question of *why* (or if) privacy is valuable. For example, while philosophers have argued that privacy is necessary for developing identity,[4] or for autonomy,[5] economists—primarily concerned with

[1] Privacy 2018 (Search Term), GOOGLE NEWS, https://www.google.ca/search?q=privacy+2018&source=lnms&tbm=nws (last visited Apr. 21, 2018).

[2] *See* DANIEL SOLOVE AND ALAND SCHWARTZ, INFORMATION PRIVACY LAW 807 (6th ed. 2017); *id.* at 811 ("standing has been a particularly challenging issue in privacy cases, with many such cases being dismissed for lack of standing because of courts concluding that plaintiffs have not suffered harm."); *see also In Re* Google Inc. Privacy Policy Litigation, 2013 WL 6248499 (N.D. Cal. 2013); Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc., 528 U.S. 167 (2000) (ruling that the standing doctrine requires injury in fact, and such injury must be concrete, particularized, and actual or imminent).

[3] In this Article, we use "privacy" to refer to information privacy.

[4] *See* Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. PUB. AFF. 26 (1976); JOSEPH BENSMAN & ROBERT LILIENFELD, BETWEEN PUBLIC AND PRIVATE: THE LOST BOUNDARIES OF THE SELF (1979).

[5] *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); *see also* STANLEY BENN, PRIVACY, FREEDOM AND RESPECT FOR PERSONS, *in* PRIVACY: NOMOS XIII 8 (Ronald Pennock & John Chapman eds., 1971).

efficiency—have tended to perceive privacy as a means of concealment,[6] and argue that privacy is a source of inefficiency.[7]

The second approach, which is more popular in legal scholarship, sidesteps this more elementary normative question and, taking the value of privacy as a given, moves directly to questions of degree and manner: to what extent should privacy be protected, and what form should these protections take? This has often included suggesting a property right protection over personal data.[8]

We aim to bridge this divide. We begin by assuming that, in addition to privacy's instrumental value (for example, to avoid the financial burdens of identity theft), a diminution of privacy, which we call privacy loss, can also create a unique type of injury, which we call privacy harm.[9] Think about a friend who puts a sticker on her laptop's webcam, a colleague who does not use social media because he thinks it entails "too much sharing," or a family member who uses an end-to-end encrypted messaging app. Putting aside the possible fear that this information could be used against them, these decisions reflect that fact that, in the absence of these precautions, these individuals would suffer some disutility. This disutility is relevant for the law.

We model privacy loss in a manner that is consistent with the three dominant conceptions of privacy: access (the law and economics conception of privacy as concealment), control, and context. Our model defines privacy as the standard deviation of the probability distribution around a mean representing a person's type—the information that another person wants to find out about her. In this model, when a person attempts to learn personal information about someone else, he observes a random draw from a distribution centered at the "true value" of that

[6] *See, e.g.*, Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. PAPERS & PROCEEDINGS 405 (1981).

[7] An exception to this is intellectual property.

[8] *See, e.g.*, James Rule & Lawrence Hunter, *Towards Property Rights in Personal Data*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 168 (Colin J. Bennett & Rebecca Grant eds., 1999); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. PRAC. 56 (1999); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1 (1996); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056 (2004).

[9] M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1131, 1142–55 (2011) (separating between subjective privacy harms, which we focus on, and objective privacy harms, which refer to other interests being harmed through the coerced or unanticipated use of someone's information against that person); *Cf.* Lisa Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 131 (Austin Sarat ed., 2015) (arguing that privacy law should move from the paradigm of harm and consent to one of power).

information. After aggregating these draws with his prior, he forms a subjective distribution, which represents his new, better-informed beliefs. Privacy corresponds to the standard deviation of the distribution. To this, consistent with the legal and philosophical approaches, we add an intrinsic desire for privacy. This addition moves the model from the realm of privacy as concealment to the realms of privacy as control and privacy as contextual integrity.

Our model contributes to existing privacy scholarship in two ways. Like other economic analyses, our model has the benefit of being concrete and tractable. However, because it does not view the loss of privacy as dichotomous, our approach can handle variations of degree: our proposal is the first in this literature to model privacy as a continuum. Given that privacy is not binary, privacy loss and privacy harm should not be binary either.[10] It also contributes to the law and economics of privacy literature. While we do not diminish the argument that individuals might value privacy because it allows them to conceal undesirable facts about themselves, we add a second motivation to the model: that, at least in certain contexts, individuals *like* privacy. This model is the first in this literature to take intrinsic privacy preferences into account. In this regard, our approach is closer to that employed by most of the legal privacy scholarship.[11]

We then apply the model to two central areas of privacy law: the common law privacy tort and the Fourth Amendment third party doctrine.[12] In the tort law context, our proposal helps to clarify the existing common law doctrine by better distinguishing privacy harms from reputational harms. By clarifying the underlying interests protected by the privacy tort, it also suggests a need to reevaluate current evidentiary standards and the relationship between the First Amendment and the privacy tort.

[10] Some courts have recognized that privacy does not work as a binary concept. *See* Sanders v. ABC, 978 P.2d 67 (Cal. 1999) ("privacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy").

[11] Our model does not attempt to capture every nuance of privacy in the real world. Rather, our goal is to create a model that captures the most important aspects of privacy, in order to gain insights about how privacy is, and ought to be, handled by the legal system. Like a law school hypothetical, a model helps to clarify fundamentals by stripping away all the surrounding brush to reveal the root of the concept.

[12] *See* Lisa Austin, *Privacy and the Question of Technology*, 22 L. & PHIL. 119, 164 (2003) (arguing that, "we do not need to invent a new theory of privacy from the ground up in order to deal with the threats posed by information technology. However, because technology creates privacy issues that appear to fall outside the bounds of our traditional analysis—known and even accepted surveillance, collection of non-intimate information, collection of information in public—we do need to sharpen and deepen our understanding of traditional concerns regarding privacy in order to respond to these new situations.").

In the Fourth Amendment context, our proposal illuminates the inherent mistake of the discredited—but still commonly applied—third party doctrine: its inability to see privacy in a non-dichotomous way. This, we argue, mistakenly turns the Fourth Amendment's "reasonable expectations of privacy" test into a strict liability rule. Based on our model, we propose a way to conceptualize the "reasonable expectation of privacy" test by turning it into a negligence rule that is more appropriate given the aims of the Fourth Amendment.

We develop our approach as follows. In Part I, we describe the problem of defining privacy loss by outlining the different definitions of privacy. In Part II, we present our model of privacy loss. We then apply our model to the common law privacy tort in Part III. In Part IV, we discuss the implications of our model for the Fourth Amendment third party doctrine. The Appendix to this Article contains the mathematical formalization of the model presented in Part II, as well as some mathematical extensions.

I. THE PROBLEM OF PRIVACY LOSS

A. NORMATIVE CONCEPTS OF PRIVACY

Judith Jarvis Thomson famously observed that "[p]erhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is."[13] In the forty years since she made this observation, the literature has made little progress on this front. Helen Nissenbaum, accordingly, has noted that "[o]ne point on which there seems to be near-unanimous agreement is that privacy is a messy and complex subject."[14] Robert Post has gone even further, remarking that "[p]rivacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."[15]

Daniel Solove, for example, has identified no less than six distinct ways to conceptualize privacy: as (1) the right to be let alone, (2) autonomy or the limited access to the self, (3) secrecy or concealment of discreditable information, (4) control over one's personal information, (5) personhood and preservation of one's dignity, and (6) intimacy and the promotion of relationships.[16] While this classification is widely

[13] Judith Jarvis Thomson, *The Right to Privacy*, 4 PHIL. PUB. AFF. 295, 295 (1975).

[14] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 67 (2010).

[15] Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087 (2001).

[16] Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1099–21 (2002).

accepted,[17] it is not universal. Across these different normative conceptions, the term "privacy" typically refers to the control of one's personal information, or as limiting access to such information. More recently, scholars have begun to adopt a conception of privacy that centers around the contextual integrity of personal information.[18]

The intellectual roots of the common law right to (informational) privacy can be traced to an 1890 article by Warren and Brandeis.[19] In it, they characterize the right to privacy as the "right to be let alone," and demonstrate that this right, although not formally recognized under the Common Law, was already widely acknowledged and protected.[20] Unlike prior authors, who had argued for enhancing privacy as a defense against State intervention, Warren and Brandeis were primarily concerned with intrusions by other private parties. Like many today, their concern about privacy was spurred by a recent technological innovation. In their case, this innovation was the camera, which had dramatically reduced the cost of capturing people's image.

Others come at privacy from a different angle, arguing instead that privacy is a necessary tool for the promotion of individual autonomy. A lack of privacy can lead an individual to feel (rightly or wrongly) that she is constantly under scrutiny by others. As a result, the absence of privacy constrains the spectrum of thoughts and behaviors that she considers acceptable and limits her freedom to fully develop as an autonomous person.[21] Proponents of this conception of privacy focus on an individual's ability to limit access to her person, and argue that doing so requires three elements: secrecy, anonymity, and solitude.[22] Because these three elements are jointly necessary and sufficient, none of them alone can encompass privacy interests. Instead, a loss of any of them is a privacy loss, even if the other two remain protected.[23]

Posner, on the other hand, famously argued that privacy is mainly a matter of concealing undesirable facts about oneself. This concealment can take two forms. First, an individual can hide unflattering information about herself: information that would lower the receiver's opinion of

[17] *See, e.g.*, Richard B. Bruyer, *Privacy: A Review and Critique of the Literature*, 43 ALBERTA L. REV. 553 (2006).

[18] *See* NISSENBAUM, *supra* note 14, at 69–71; *see also infra*, Subpart I.B.

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

[20] *Id.* at 205.

[21] *See, e.g.*, Cohen, *supra* note 5, at 1377; Benn, *supra* note 5.

[22] Reiman, *supra* note 4.

[23] SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION (1989); DAVID M. O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY (1979); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980); Edward Shils, *Privacy: Its Constitution and Vicissitudes*, 31 L. CONTEMP. PROBS. 281 (1966).

her.[24] For example, concealing the fact that one has been convicted of a crime. An individual can also conceal information by a second, more subtle means, by failing to correct a misunderstanding or misperception. For example, she might prefer not to divulge a serious health problem to an employer.[25] With respect to this second type of concealment, Posner adds that an individual might choose to reveal information selectively without strictly lying or deceiving,[26] and that individuals are always eager to disclose facts that portray them in a positive light. In short, a fair evaluation of Posner's conception of privacy is that it exists mainly as a device to deceive: to create or maintain a false impression.

In contrast, some view privacy as simply control over one's personal information. A refined notion of an individual's level of privacy, they argue, shows that privacy is not the absence of information about her in public (as in Posner), but rather the control that she has over that information.[27] Privacy has also been defined along these lines as the absence of undocumented personal knowledge.[28]

In a similar vein to those who view privacy as autonomy, the defenders of privacy as personhood argue that privacy is central to developing one's own identity.[29] Paul Schwartz, for example, criticizes the paradigm of control over personal information as a view that mistakenly takes autonomy as a given, and argues that privacy is intrinsically linked with self-determination.[30] Agreeing to terms and conditions, for example, might technically fall within control over one's personal information, but could nevertheless violate one's privacy because the terms and conditions can contain boilerplate terms that the user does not understand.

Finally, supporters of privacy as intimacy argue that the concept of intimacy encompasses all the types of information that an individual

[24] Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 394 (1978); Posner, *supra* note 6, at 405.

[25] Posner, *The Right of Privacy*, at 394; Posner, *supra* note 6, at 405.

[26] Posner, *supra* note 6. For example, most people present themselves differently to their partners than they do to their employers. Rather than being considered deceitful, we generally refer to this as acting professionally.

[27] Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News, and Social Change*, 1890-1990, 80 CALIF. L. REV. 1133 (1992); Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968) ("[P]rivacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves."); Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1464 (2000); *see also* ALAN WESTIN, PRIVACY AND FREEDOM (1967).

[28] W.A. Parent, *A New Definition of Privacy for the Law*, 2 L. PHIL. 305 (1983); William Parent, *Privacy, Morality, and the Law*, 12 PHIL. PUB. AFF. 269 (1983).

[29] Reiman, *supra* note 4; BENSMAN & LILIENFELD, *supra* note 4.

[30] Schwartz, *supra* note 8. Schwartz, for example, criticizes the paradigm of control over personal information as a liberal view that mistakenly takes autonomy as a given, and argues that privacy is intrinsically linked with self-determination.

would rather keep private. They see privacy is a tool to protect the individual from being subject to misrepresentations that could occur when others know some pieces of information about her out of context, which could lead to misunderstandings.[31] The right to privacy defines information territories: places where it is socially acceptable to keep or to disclose information, and which define the boundaries of private life and social life.[32]

B. DESCRIPTIVE CONCEPTS OF PRIVACY

While some authors' conceptualizations of privacy fit neatly into one of the six categories, others do not.[33] This is because the conceptions of privacy discussed above are not mutually exclusive. For example, while some focus on the ultimate goals of privacy, others are more concerned with how it is protected. Control over personal information, for example, can be seen as derivative of the limited access to the self. Limited access to the self, in turn, is in many ways similar to the right to be let alone, and the creation of the self seems like a combination of the two. What they all have in common is that they conceptualize privacy by looking for a necessary and sufficient set of elements and, in such way, find its "essence."[34]

The normative approach leads to two difficulties. First, it ignores the basic intuition that "privacy" depends on both facts (including cultural, historical and technological facts) and context, not only on some essential characteristic.[35] Second, many of the concepts that are used to define privacy are themselves hard to pin down. While these can be useful

[31] Robert S. Gerstein, *Intimacy and Privacy*, 89 ETHICS 76 (1978); James Rachels, *Why Privacy Is Important*, 4 PHIL. PUB. AFF. 323 (1975); JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION (1992).

[32] Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957 (1989).

[33] For example, some conceptualizations of privacy seem to fit into more than one category. At the same time, others, such as Nissenbaum's privacy as context, do not fit naturally into any of them. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004); *see also* Adam Barth et al., *Privacy and Contextual Integrity: Framework and Applications*, *in* 2006 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (2006), http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1624011.

[34] Solove, *supra* note 16, at 1096 (noting that all approaches fail for being both under and over inclusive, and abandoning the search for a definition of privacy); *see also* NISSENBAUM, *supra* note 14, at 68:

> [S]ome authors have argued that confusion over the concept of privacy arises from a failure to recognize the difference between descriptive or neutral conceptions and normative ones. To provide a neutral conception is to state what privacy is without incorporating into its meaning that privacy is a good things, worth having, and deserving moral and legal protection . . . One of the benefits of starting with a neutral conception of privacy is that it allows one to talk about states of increased and decreased privacy without begging the normative question of whether these traits are good or bad.

[35] NISSENBAUM, *supra* note 14.

for linking privacy breaches to situations that people intuitively consider wrongful,[36] their primary contribution is not to provide a sharp boundary. For example, autonomy and personhood have many facets and are no easier to define than privacy itself. Someone suffering from a privacy violation might complain that such violation injures her personhood or autonomy, but this statement does little to pin down the circumstances under which an individual loses privacy.[37] These difficulties are so acute that Post has argued that it is extremely difficult, if not impossible, to succeed in this endeavor of defining the right to privacy's essence.[38]

In contrast to the six normative conceptions of privacy, we can think of three descriptive conceptions of privacy: limiting access to personal information, control over information, and appropriate information flows.[39] Because these views aim to identify when privacy is diminished, rather than when privacy rights are breached, they relate more closely to identifying harms to privacy. The discussion above makes clear that one way to interpret the perspective of those who advocate for privacy as the right to be let alone or for privacy as secrecy is that they operate under a logic of access, while we can see most of the proponents of privacy as autonomy or as control as operating under the logic of control, and most of those who view privacy as personhood and intimacy doing so based on a logic of information flows. As we discuss in more detail below,[40] our model can be interpreted in light of any of these three descriptive conceptions of privacy.

Rather than aiming to define privacy, we offer a functional model of privacy that is designed for legal analysis.[41] While our proposal is compatible with these previous approaches, our goal is to develop a model that is both simple to apply and useful for legal analysis. As Ryan Calo has said, "describing the outer boundaries and core properties of privacy harm helps to reveal values, identify and address new problems,

[36] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

[37] *Id.*

[38] Post, *supra* note 15.

[39] NISSENBAUM, *supra* note 14, at 67–126.

[40] *See* Subpart II.B.

[41] *Cf.* NISSENBAUM, *supra* note 14, at 68:

> [O]ne of the benefits of starting with a neutral conception of privacy is that it allows one to talk about states of increased and decreased privacy without begging the normative question of whether these states are good or bad. It leaves open the possibility that in certain circumstances less privacy might be better than more and that reductions in privacy need not constitute violations.

and guard against dilution."[42] In the following Part, we aim to describe such boundaries.[43] We do so with a model that captures the idea that information privacy is about people's ability to deduce our personal information, which underlies each of the three descriptive approaches to privacy discussed above.[44]

II. THE PRIVACY BELL

We model an individual's level of privacy with respect to how certain an outsider is about fundamental aspects of that individual. The more certain the outsider is about the individual's attributes, the less privacy the individual has with respect to him. As a result, such an increase in the outsider's certainty corresponds to a privacy loss to the individual.

We formalize this concept in a tractable model. We then take this model of privacy loss and apply it to contexts in which the law protects privacy. Since the law typically does so in contexts where individuals *like* privacy, we embed our model of privacy loss into a setting where, other things equal, an individual prefers more privacy to less.[45] By combining these two building blocks, our model can be applied to a wide variety of legal contexts. We illustrate the value of this formalization below,[46] where we apply it to central issues in privacy law and show how the formalization presented here provides new insights to doctrinal debates.

A. PRIVACY LOSS

Consider an individual named Abby. Abby has a fundamental characteristic. This might be her willingness to pay for a good, her wealth, her desirability as an employee, or her intrinsic worth as human being. We will refer to this as her "type." Initially, only Abby knows her type. For the purposes of this example, we will suppose that Abby's type represents her desirability as an employee.

Now consider Ben. Ben is considering hiring Abby, and would like to know how desirable Abby is as an employee. Ben cannot observe

[42] *See* Calo, *supra* note 9, at 1142; *see also* Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361 (2014).

[43] *See* Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 234 (1977) (arguing that privacy will be important and worthy of protection only when its concept is more clearly delineated, and stating that "a legal concept [of privacy] will do us little good if it expands like a gas to fill up the available space").

[44] *See* NISSENBAUM, *supra* note 14, at 68 ("[T]hose, like Gavison, who propose a neutral conception do not deny the possibility of normative accounts of privacy.").

[45] In the mathematical appendix, we also consider the standard setting in which individuals have utility that is increasing and concave in privacy. In other words, we assume that she likes privacy, and values an incremental amount of privacy more when she has little of it left than she does when she has a lot of it.

[46] *See infra* Parts III, and IV.

Abby's type directly. However, Ben does have a fairly good idea about what the overall population of workers in the community looks like. He knows, for example, how productive the average worker is. He also knows the general shape of the distribution—for example, whether workers are evenly spread out across different types, or whether they tend to be bunched together with only a few outliers.

Ben can also observe signals, or clues, that allow him to guess something about Abby's type. For example, while he may not know exactly how desirable she is as an employee (her "type"), he may be able to learn where she went to college, how many jobs she has had in the last year, and whether she has ever been convicted of a felony. None of these signals fully reveal Abby's type (her desirability as an employee) on their own. They do, however, allow Ben to form a clearer picture about it. Specifically, when he aggregates these signals, Ben can form his best guess about Abby's type. Because he knows that this is only an informed guess, he still has some uncertainty about her type—he might guess too high or too low. The more uncertain Ben is about Abby's type, the more privacy she has.

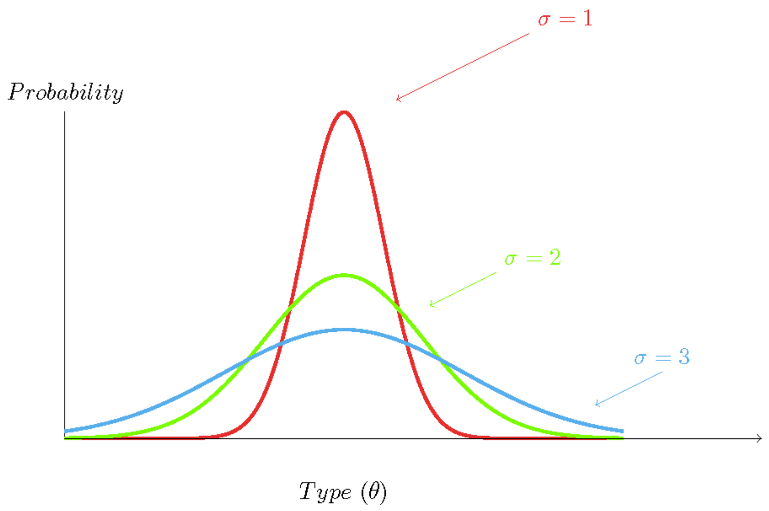

Figure 1: The Privacy Bell: Abby's privacy is higher when the distribution has fatter tails.

Figure 1 illustrates this intuition. When Ben has few signals about Abby's type (σ=3, the blue curve), he knows that there is a wide range of types that are plausible. As he gets to know Abby better (moving from the blue curve to the green curve, σ=2), the distribution becomes narrower, meaning that the range of plausible types narrows. As he gets to know Abby better still (moving to the red curve, σ=1) Ben has a good idea about what he wants to know about Abby: the odds that Abby's type is way out in either tail diminishes dramatically, and there is a narrower range of plausible (or likely) values.[47]

In the figure above, we assume that each signal is drawn from the same distribution. We would expect that, most of the time, the first signal to have the greatest effect on Ben's posterior. This makes intuitive sense—just like a first impression, the first thing Ben learns about Abby is likely to have a big impact on his beliefs.[48]

While we leave the formalization of our model to the Appendix,[49] the intuition behind the model is simple. As Ben learns things about Abby, he gets a better sense of who she is. When he does so, Abby loses some privacy. Each time Ben observes another signal about Abby, he becomes more certain about her type. Every increase in his certainty results in an equivalent privacy loss to Abby. Mathematically, Ben's certainty increases because the standard deviation of his Bayesian posterior falls. Because this incremental increase in Ben's certainty and loss of Abby's privacy are two sides of the same coin, it is natural to model privacy loss as the reduction in the standard deviation of Ben's posterior (the Bell curve illustrated in Figure 1).[50]

In the real world, not every piece of information is created equally. For example, in the context of Abby's health, learning that she had a mild cold last winter is not the same thing as learning the detail of her family's medical history. This can be captured in our model by allowing different

[47] We use the term "plausible" loosely. Strictly speaking, in the example illustrated in Figure 1, all values along the x-axis remain possible, even for the red curve. The difference between the curves is that the likelihood of a value far from the center of the distribution is lower under the red curve than it is for the blue one. Because the likelihood of such a value is very low, we can think of these values as being implausible, even if they are possible.

[48] *But see infra* notes 51–52.

[49] *See infra* Part V.

[50] In addition to observing signals—which convey a fact—it is possible for a fact to be "common knowledge." Formally, if a fact is "common knowledge" among a group of people, it does not only mean that everyone knows the fact. It also means that everyone knows that everyone knows the fact, and that everyone knows that everyone knows that everyone knows it, and so on *ad infinitum*. *See, e.g.*, DREW FUDENBERG & JEAN TIROLE, GAME THEORY 4 (1991). Our model does not distinguish between signals that everyone has observed and signals that are common knowledge in this formal sense. While we would interpret both situations as involving the same level of privacy, they may have different implications for the individual whose privacy is implicated, since the two situations might lead observers to act in different ways. In other words, while common knowledge does not affect Abby's level of privacy directly, it might change how Ben acts in the face of knowledge about Abby.

signals to have different amounts of informativeness, as there is nothing in the model that requires each fact to be treated equally.[51]

A common example in the privacy literature is the naked body.[52] To build on this familiar example, suppose Douglas and Evan are playing strip poker. Because Douglas is a much better poker player than Evan, Evan is repeatedly required to remove articles of clothing. Each article he removes can be interpreted as sending a signal to Douglas about what his naked body looks like. If the first article Evan removes is a sock, this is not very informative—Douglas learns very little from observing Evan's bare foot. Eventually, Evan removes his sweater, which send a stronger signal to Douglas. However, if Evan had previously forgotten about his watch, and removes it next, this signal would not be very informative. If the game continues, and at some point Evan removes his shirt, this would send a very strong signal to Douglas. In this example, each signal carries a different amount of information. Moreover, the informativeness of each signal depends on the prior signals that Douglas has received (for example, removing his right sock than it would be if he had not already done so).[53]

For the purposes of the model, we assume that an individual's type can be summarized by a point on some unidimensional interval *I* (the x-axis in Figure 1). This restriction is an expositional convenience.[54] This does not imply that type summarizes only one category of information. Just as the price of a car summarizes a host of factors about the vehicle itself, as well as factors related to the local market and, in certain cases, the buyer, an individual's type can be interpreted as a summary of all relevant information about her for the purposes for which the acquirer gathers her information.

In our model, privacy exists on a continuum, meaning that Abby's level of privacy can increase or decrease, and can increase or decrease by varying amounts. We believe that this represents an improvement over a dichotomous model in which people just "have" or "do not have" privacy

[51] Indeed, some signals might have no informativeness at all, just as some facts might be completely useless in answering a particular question. These signals would have no effect on Ben's posterior. It is also possible that Ben could learn things that are contradictory, which could actually lead him to become less certain about Abby. While that is true—both intuitively and in the mathematical formalization—we focus in the more common situation in which more information leads to a clearer picture. This corresponds to a situation in which more signals lead to a tighter posterior distribution.

[52] *See, e.g.*, Yofi Tirosh & Michael Birnhack, *Naked in Front of the Machine: Does Airport Scanning Violate Privacy?*, 74 OHIO STATE L.J. 1263, 1265 (2013).

[53] We explore some of the implications of aggregating signals in the context of ISPs in a companion paper. *See* Ignacio N. Cofone & Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L.J. (forthcoming Aug. 2018).

[54] We relax this assumption in the Appendix, Subpart B.3.

for two reasons. First, we believe that it better captures the basic intuitions of privacy. Informational privacy is not only about having privacy or not. When Ben learns a fact about Abby, it is not that Abby no longer has *any* privacy, nor is it true that before that, she had "full" privacy. Instead, informational privacy is really about *levels* of privacy. When Ben learns about a fact about Abby, her level of privacy falls. He doesn't know *all* the facts about her, and it would be absurd to say that she no longer has *any* privacy. But nor is it correct to say that nothing has happened with respect to her privacy. Instead, it is most appropriate to simply say that her level of privacy has declined.

Second, the continuous nature of privacy in our model allows it to better capture the tradeoffs associated with privacy and privacy law. Whereas dichotomous conceptions allow only for two possible outcomes, "privacy breach" and "no privacy breach," our model is better suited for "grey areas" where careful and rigorous analyses are most useful and needed. We discuss some such grey areas below in Parts III and IV.

B. Preferences Over Privacy

1. People May Desire Privacy

The second building block deals with how Abby feels about this privacy loss. In other words, we define Abby's preferences over privacy. Because our primary goal is to apply our model to contexts in which the law engages with informational privacy, we will use it in contexts where Abby likes privacy.[55]

What does this model imply about the reasons for which people desire privacy? First, as discussed above, the model captures the idea that individuals have an intrinsic desire for privacy; It's that people also desire

[55] We model this preference in the most standard way possible. We assume that individuals like privacy in most contexts and, all other things equal, they like more privacy better. This is not to say that there are no other settings in which an individual might feel differently. Indeed, it does not take a psychologist to know that in some settings, individuals *like* to share details about themselves with third parties. For example, Abby might enjoy sharing details about her day with her spouse or friend, and it might make her happy to know that her loved ones have a very clear sense of her type (such as, that they know her very well). While we recognize that these settings are important, they are not the types of settings in which the law engages with informational privacy, and are therefore not the primary focus on this Article. Even in such settings, however, the first part of our model—the model definition of privacy loss—is still valid, and can provide a useful framework for formal analysis. This is also not to say that individuals never value privacy for instrumental reasons. Just as a person might want to eat apples both because they taste good and because they are good for one's health, a person might want to maintain privacy both for intrinsic and instrumental reasons.

In the mathematical formalization in the Appendix, we add the very standard assumption that, like most good things in life, privacy has diminishing returns. Abby will mind it less that Ben finds out a little about her when Ben knows almost nothing about her, than she will when Ben has already found out a lot about her. Figure 2, in the Appendix, illustrates an example of such a utility function.

privacy for its own sake.[56] This is not to say, however, that they cannot also desire privacy for instrumental reasons. For example, in addition to valuing privacy for its own sake, Abby might value privacy because it allows her to conceal unflattering facts about herself, or because it protects her from suffering financial harm. In this sense, this model is not inconsistent with the economic conception of privacy.[57] Rather, this conception can be captured within the model by setting the marginal utility of privacy to zero for all levels of privacy.

Second, while this conception of privacy is intrinsic—in the sense that individuals desire privacy for its own sake—it captures the fact that individuals can, and do, trade (or sell) their privacy for other goods or services.[58] Abby will face a privacy loss when she shares information, but her overall utility might still increase given the benefits that she obtained due to sharing it. Abby's utility will also depend on how Ben uses her information, but those harms are best conceptualized not as privacy losses, but as other losses that were enabled due to a loss in privacy[59]—what Calo has called extrinsic privacy harms.[60] Moreover, because it conceives of privacy along a continuum rather than as a dichotomy, as discussed above, we can also model individual preferences over privacy as a continuum. This captures the idea that giving up a small amount of privacy is different from a large privacy loss.

In principle, the tighter Ben's posterior distribution, the less privacy Abby will have and, all else equal, the less utility she will have.[61] That said,

[56] Calo, *supra* note 9 (internal quotation marks omitted) (explaining that:

> [P]rivacy harms fall into two categories. The first category is 'subjective' in the sense of being internal to the person harmed. Subjective privacy harms are those that flow from the perception of unwanted observation. Subjective privacy harms can be acute or ongoing, and can accrue to one individual or to many. They can range in severity from mild discomfort at the presence of a security camera to mental pain and distress far greater than could be inflicted by mere bodily injury.).

[57] *See supra* INTRODUCTION.

[58] *But see* Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95 (2013) (arguing that it is misleading to say that internet users "pay" for goods and services with their data because there is no functioning market for personal information exchanges).

[59] Of course, if Ben sells or gives information to other parties, these would also be privacy losses. We address this in Part III.A, *infra*.

[60] Calo, *supra* note 9, at 1143:

> Objective privacy harm is the actual adverse consequence—the theft of identity itself or the formation of a negative opinion—that flows from the loss of control over information or sensory access. Subjective privacy harm is, by and large, the perception of loss of control that results in fear or discomfort.

[61] Of course, Abby's disutility also depends on who Ben is to Abby. Abby might experience a negligible utility loss from her partner learning something about her. Indeed, as explained infra, this might even lead to a utility gain. On the other hand, she may experience a significant utility loss if the same fact became known to a stranger in the street.

there will be situations in which privacy loss will be more complex. In many situations, Abby's marginal utility of regarding privacy will be flat, rather than increasing. Those who believe the "I have nothing to hide" argument claim to have no privacy disutility from affirmatively sharing information with others. This might be the case. If so, they might even pursue sharing information, with a consequential privacy loss, because they suffer no harm from the loss of privacy, while the act of sharing brings them benefits—which can range from material benefits to gains in intimacy or agency.[62] In other words, they are able to selectively reveal information. We view these not as privacy gains, but rather as extrinsic privacy gains that accrue as a consequence of a reduction in privacy.

Moreover, depending on the one's conception of privacy, one will have a different reading of this model. A proponent of the privacy as secrecy or control approach might interpret a privacy loss as the reduction in the probability distribution, independent of the subject's utility. When Ben learns more about Abby, she has less secrecy and less control over her information, even if she is not unhappy about this loss. Alternatively, a proponent of the privacy as contextual integrity approach[63] might focus on the reduction in marginal utility, because it is this reduction that indicates that, given the context, her information flowed in a socially inappropriate manner. If Ben learns more about Abby and she does not mind it, this implies that Ben learned the information through a socially appropriate channel.

2. *Preferences over Privacy vs. Preferences over Signals*

It is worth noting the distinction between Abby's preferences over *privacy* (such as, the standard deviation of Ben's posterior) and her preferences over *information*. In our model, Abby cares about the latter only to the extent that it affects the former.

This is the case with respect to both the level of her utility and to the function's shape. For example, while Abby's utility over *privacy* may be concave (implying that she values privacy more when she has very little of it), her utility over *information* may not be. This is because the more Ben already knows about Abby, the less effect any particular signal will have on the standard deviation of his Bayesian posterior.

As a result, while the first few signals affect the *standard deviation* a lot, Abby's preferences are such that a reduction in standard deviation from a high starting point has a relatively small effect on her *utility*. This

[62] *See supra* note 45.

[63] *See* NISSENBAUM, *supra* note 14.

is because, at that high starting point, she already has a lot of privacy, so losing a little might not be painful to her.

To see how this works, consider Bill Cosby. According to an article in *The Guardian*, by December 31, 2015, Cosby had been accused of sexual abuse, harassment and/or attempted abuse by 57 different women.[64] While the first allegation was reportedly made to the police in March 2000, victims' stories did not receive widespread media attention until Joan Tarshish's interview on CNN.[65] This allegation opened the floodgates, and by the end of November, 14 more women came forward. The media attention around Cosby was intense,[66] and the episode prompted substantial amounts of soul searching.[67] A man who was once beloved as "America's Dad"[68] has now become the butt of the jokes of one of his onetime admirers.[69] We can think of these allegations as signals. While the first few allegations made a huge impact on the way people saw Cosby, it is fair to say that as the number of accusers continued to swell, the *marginal* effect of each additional accusation began to shrink. Once ten women had accused Cosby of assault, the eleventh allegation, on its own, is unlikely to have much of an effect of an observer's posterior. This is not to say that a trial is unnecessary, only that the effect of an additional *allegation*, without more, is likely to be smaller.

C. Privacy Versus Reputation

So far, we have been assuming that Ben had, on average, the right idea about Abby. In other words, we have been assuming that the mean of his prior distribution was equal to the true mean. Moreover, thus far, we have been assuming that when Ben observes signals about Abby, those signals are themselves unbiased—and that they are, on average, correct. As a result, when Ben observes additional signals about Abby, their primary effect on his posterior is on its standard deviation. Indeed, on average, they have no effect on the mean of his posterior.

[64] Amanda Holpuch, Jessica Glenza & Nicky Woolf, *The Bill Cosby Sexual Abuse Claims—57 Women and the Dates They Went Public*, GUARDIAN (Dec. 31, 2015, 1:03 PM), https://www.theguardian.com/world/2015/dec/31/bill-cosby-sexual-abuse-claims-57-women-dates-public-accusations.

[65] Interview with Joah Tarshish with CNN (Nov. 18, 2014, 5:01 PM), https://www.cnn.com/2014/11/17/showbiz/bill-cosby-new-accuser-allegation/index.html (last visited Apr. 21, 2018).

[66] *Id.*

[67] *Id.*

[68] Tim Walker, *Bill Cosby: The Rise and Fall of 'America's Dad'*, INDEPENDENT (Dec. 30, 2015, 8:15 PM), http://www.independent.co.uk/news/people/bill-cosby-the-rise-and-fall-of-america-s-dad-a6791381.html.

[69] Mallory Carra, *Dave Chappelle's Bill Cosby Jokes from 'The Age of Spin' Are Brutally Honest About How Former Fans Feel*, BUSTLE (Mar. 22, 2017), https://www.bustle.com/p/dave-chappelles-bill-cosby-jokes-from-the-age-of-spin-are-brutally-honest-about-how-former-fans-feel-45800.

Not all information has this attribute. Of particular interest in the privacy context is what we might call "left field" information —information about Abby that Ben never even thought to think about. For example, consider the allegation that the former UK Prime Minister David Cameron engaged in bestiality while at university.[70] To most people, this allegation came out of left field—it seems safe to say that the average person had never given any thought to the possibility that Cameron may or may not have engaged in bestiality. Had Angela, one such person, been asked about it, she would likely have answered that the odds of him having done so were infinitesimally small.

The publication of the allegation was a signal about Cameron. While Angela might not have known for certainty whether the allegation was true, we can interpret the allegation as increasing her subjective probability that Cameron had engaged in bestiality. The signal actually made Angela *less* confident about Cameron's type—whereas before she was almost certain that Cameron had not engaged in bestiality, now she is less certain. As a result, to the extent that his engagement is bestiality is relevant to Angela's evaluation of Cameron's type, this would in turn make Angela more uncertain. The standard deviation of her posterior would therefore *increase*, not decrease. In the context of our model, this implies that Cameron has *more* privacy, not less.

While this may seem problematic, it actually points to a deeper insight captured by the model: the relationship between reputation and privacy.[71] In addition to causing her posterior to widen, to the extent that Angela thinks that bestiality is an undesirable attribute, this increased probability would cause Angela's subjective posterior distribution of Cameron's type to shift to the left. This is the equivalent of a reputational hit to Cameron. We will come back to this distinction below, where we discuss the application of the model to tort law.[72]

The key point is that the allegation of bestiality resulted in Angela becoming less confident about Cameron—the standard deviation of her posterior is wider. As a result, from Angela's perspective, she knows *less* about Cameron then she did before, even though she has observed an additional signal about him. This is the case even if the allegation is true.

[70] Nadia Khomami, *David Cameron, a Pig's Head and a Secret Society at Oxford University—Explained*, GUARDIAN (Sept. 21, 2015, 9:29 AM), https://www.theguardian.com/politics/2015/sep/21/david-cameron-piers-gaveston-society-what-we-know-oxford-secret.

[71] *See* Andrew F. Daughety & Jennifer F. Reinganum, *Public Goods, Social Pressure, and the Choice between Privacy and Publicity*, 2 AM. ECON. J.: MICROECONOMICS 191, 191 (2010) (introducing a model where individuals suffer reputational harm from the loss of privacy, so privacy protection allows them to engage in an optimal level of activity).

[72] *See infra* Part III.

This example also illustrates how, under certain circumstances, a person might experience a utility gain from a reduction privacy. Suppose that the allegations about Cameron's bestiality were false. Once the (false) allegations are made public, Cameron's best strategy might be to quickly reveal his non-bestiality type to the world. While he would suffer a privacy loss by doing so, the reputational benefit that he experiences would more than make up for it. He would therefore be happy to have a tighter Bayesian posterior.

In the next Part, we apply this model to the first of two areas of law—the privacy tort. In doing so, we further draw out the distinction between a privacy interest and a reputational interest. These two interests, while related, are also distinct.

III. Tort Law Doctrinal Consequences

A. Privacy's Two Protected Interests

The common law privacy tort has four facets: (1) appropriation of one's name, image or likeness ("appropriation"); (2) false light; (3) intrusion upon seclusion ("intrusion"); and (4) public disclosure of private facts. The first of these, appropriation, allows an individual to prevent the use of her name and picture for commercial purposes (including advertising) without her consent. False light is implicated when a third party uses true facts to create a false impression. Intrusion upon seclusion gives an individual the right to prevent third parties from obtaining information about her by intrusive means. Finally, public disclosure of private facts allows her to prevent the publication by a third party of intimate facts about herself.

While the term privacy typically involves the control of, limited access to, or contextual integrity of personal information,[73] the privacy tort has long been known to defend wider interests. Post has noted that privacy attempts to safeguard minimal rules of civility, protecting the identity of individuals in a community.[74] As he put it, "the common law torts of defamation and invasion of privacy represent just such efforts to use law to subject communication to 'universal' cultural standards."[75] "[I]ntentional infliction of emotional distress is one of a family of actions, which include defamation and invasion of privacy, that are designed to

[73] Solove, *supra* note 16; NISSENBAUM, *supra* note 14.

[74] Post, *supra* note 32, at 959–86.

[75] Robert C. Post, *The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and* Hustler Magazine v. Falwell, 103 HARV. L. REV. 601, 634 (1990) [hereinafter Post, *Constitutional Concept*]; *see also* Robert C. Post, *The Social Foundations of Defamation Law: Reputation and the Constitution*, 74 CALIF. L. REV. 691, 714–15 (1986) [hereinafter Post, *Social Foundations*].

protect the respect to which the law believes persons are entitled."[76] In fact, invasion of privacy has been explicitly described by the Supreme Court as a remedy for injuries "to plaintiff's emotions and . . . mental suffering."[77] This idea is also present in both Womack and in the Second Restatement of Torts, which characterize privacy, defamation and intentional infliction of emotional distress as serving two aims: the reparation of harm caused by uncivil behavior and the protection of "generally accepted standards of decency and morality that define for us the meaning of life in a 'civilized community.'"[78]

As Austin has also noted, the privacy torts protect more than just privacy.[79]

Indeed, under our model of privacy, only two of the four privacy torts truly protect privacy interests. To see this, suppose that Abby interviews for a job with Ben If Ben broke into Abby's home (intrusion upon seclusion), he would obtain *new signals* about Abby. These new signals would reduce the standard deviation of his posterior distribution of Abby's type. He could find, for example, a family picture indicating that she is caring, or a pile of dirty clothes indicating that she is untidy. This represents a loss of privacy—Ben's Bayesian posterior is tighter.

Similarly, imagine that Ben told Caroline private facts about Abby's lifestyle, something that would be actionable as a public disclosure of private facts. Our model would interpret these facts as signals about Abby. By passing these signals to Caroline, Ben is allowing *Caroline* to reduce the standard deviation of *her* posterior about Abby. Here again, Abby suffers a privacy loss.

However, Abby's privacy loss is to Caroline rather than to Ben. Ben's posterior remains unchanged, since the act of disclosing private facts to Caroline did not cause him to learn anything new about Abby. Under the privacy tort, however, Abby's claim is against *Ben*, not Caroline. This is as it should be. While the loss of privacy is to Caroline, it is Ben that *caused* Abby's loss. It is therefore appropriate for him to be the party to compensate Abby. In other words, the difference between an intrusion tort and a public disclosure tort is *whose* bell curve is narrowed by the

[76] Post, *Constitutional Concept*, *supra* note 75, at 616; *see also* Post, *supra* note 32, at 959–66.

[77] Froelich v. Adair, 516 P.2d 993, 996 (Kan. 1973); *see also* Time, Inc. v. Hill, 385 U.S. 374, 384 n.9 (1967); Post, *Constitutional Concept*, *supra* note 75, at 615.

[78] Post, *Constitutional Concept*, *supra* note 75, at 624 (citing Womack and the RESTATEMENT (SECOND) OF TORTS) (quotation marks omitted).

[79] *See* Austin, *supra* note 12, at 165–66 (arguing that many emerging issues related to information misuse, such as concern for the accuracy of information, "are *not* best described as privacy issues" and that "[t]he response to this, on my view, should not be to expand our idea of privacy to the conceptual breaking point but to clarify the many different types of interests that may be at stake in the emerging contexts of information collection, use, and disclosure.").

information. Under an intrusion tort, the perpetrator (Ben) finds reduced his probability curve of his beliefs about the target person (Abby). Under a disclosure tort, the perpetrator narrows the probability curve of a third party.

On the other hand, it is not clear how Ben's depiction of Abby to Caroline under a false light affects Abby's privacy. In our model, false light can be understood as Ben providing Caroline *false* signals about Abby. While the facts in a false light claim are themselves true, they are conveyed in such a way as to give false impression. Whether the facts themselves are true is, from Abby's perspective, irrelevant, because it is how they are *understood* by Caroline that matters. This allows us to abstract away from the facts themselves to focus on the harm that false light causes Abby. We can therefore interpret the tortious facts as false signals.

Upon receiving these false signals, Caroline's posterior about Abby will not necessarily become tighter. In fact, if the false signals are very different from Caroline's prior beliefs about Abby, they may cause her to rethink what she knows about Abby.[80] Our model captures these doubts as a widening of Caroline's posterior. In addition to widening her posterior, the misleading information might shift the mean of her posterior distribution. If we take the *x*-axis in Figure 1 to represent quality, false light might simply move the whole distribution to the left. This would cause a reputational harm to Abby, rather than a privacy harm.[81]

Finally, suppose that Caroline appropriated Abby's image and used it to advertise her company. What affect does this have on Abby's privacy? Upon seeing this advertisement, Dennis might reasonably interpret it as a signal that Abby is associated with Caroline's company or product. Of course, the fact that the image was appropriated implies that this signal is false. The fact that there may be nothing particularly damaging or embarrassing per se is irrelevant. The false signals that Dennis observes as a result of the (false) association generated by Caroline's appropriation of Abby's image still affect Dennis's posterior distribution about Abby. In particular, the most likely result of these false signals is that Dennis's posterior will become wider. Unlike false light, where the false signal would most likely lead to a downward shift is the mean of the posterior, with appropriation, Dennis's posterior could shift up or down.

[80] This situation is similar to the example of the allegations of bestiality against David Cameron, discussed above. *See supra* Subpart II.C.

[81] *See supra* Subpart II.C.

The privacy tort, in other words, protects not one, but two distinct interests: a true privacy interest, which is to protect certain aspects of ourselves from other's eyes,[82] and a reputational interest, which is concerned about one's personal image in one's community. Only the first of these, which encompasses intrusion upon seclusion and public disclosure of private facts, is a privacy interest. The second pair, appropriation and false light, relate to one's reputation. While distinct from each other, intrusion and public disclosure are both based on the idea that increasing the precision of a third party's knowledge of one's type—whether that third party is the tortfeasor—constitutes harm. For appropriation and false light, the harm is less about the standard deviation than it is about the *mean* of that distribution. In other words, the harm comes from sending misleading signals to a third party.

Therefore, while all four privacy torts center around "information about the victim," only intrusion and public disclosure refer directly to "the victim's information." This is not to say that the other two are unfounded or inappropriate. Protecting these interests through privacy law may be the most effective, and even the most coherent, method available. However, by helping to clarify the interests in play, this model can help judges determine appropriate remedies.[83]

B. AN APPLICATION TO PRIVACY'S CASE LAW

To illustrate how privacy rules are an effective means of protecting both true privacy interests and reputational interests, we turn our attention to an examination of some landmark common law privacy cases, frequently appearing in privacy law casebooks.[84] Table 1, below, shows the interests at hand in each case, according to the disputed claim.

[82] Defining privacy is more complicated than this statement suggests. *See supra* Part I.

[83] Other torts that are related to privacy but not part of the privacy tort are also about "information about the victim." Libel and slander are the most obvious of these. Indeed, under our model, libel and slander would be conceptualized in much the same way as false light. Insofar as Ben intended the reduction in Abby's privacy to cause her harm, it could be related to intentional infliction of emotional distress.

[84] *See, e.g.*, DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY, LAW ENFORCEMENT, AND NATIONAL SECURITY (2014).

	Claim	**Outcome**	**Interest**
Paveisch v. NE Life Insurance Co. (1903)	Appropriation [+Defamation]	Won appropriation	Reputation
Sidis v. F-R Publishing (1940)	PDPF	Lost PDPF	Privacy
Time v. Hill (1967)	False light	Lost false light	Reputation
Nader v. GM (1970)	Intrusion [+IIED]	Won intrusion	Privacy
Dietermann v. Time (1971)	Intrusion	Won intrusion	Privacy
Neff v. Time (1976)	PDPF, Appropriation	Lost PDPF Lost appropriation	Both
Hustler v. Falwell (1988)	Appropriation [+Defamation and IIED]	Lost appropriation	Reputation
Schulman v. GWP (1998)	PDPF, Intrusion	Lost PDPF Won intrusion	Privacy
Steinbuch v. Cutler (2008)	PDPF, False light [+IIED]	(only calls for discovery)	Both

Table 1. Common law landmark privacy cases according to their protected interests

There are two reasons why an examination of the landmark privacy cases is consistent with our argument that the privacy tort protects two distinct interests. First, as Table 1 reveals, while both interests are reflected in these cases, each case is chiefly about only one of these interests. While this is not dispositive, it supports the view that the four privacy torts can be sensibly divided into two categories along the lines that we have proposed.

Of the nine cases chosen, only two engage both interests. In *Neff v. Time* the plaintiff claimed public disclosure of private facts and appropriation.[85] In *Steinbuch v. Cutler*, plaintiff claimed public disclosure of private facts and false light (and intentional infliction of emotional distress).[86] In both cases, the plaintiff's primary claim engaged a reputational interest, with an additional claim of public disclosure of private facts to cover the facts that were appropriated and framed under a false light, respectively.

Four of the remaining cases engaged a true privacy interest. In *Nader v. General Motors*,[87] and *Dietemann v. Time, Inc.*[88] the plaintiff claimed intrusion, and in *Sidis v. F-R publishing* the claim was public

[85] Neff v. Time, Inc., 406 F. Supp 858, 861 (W.D. Pa. 1976).

[86] Steinbuch v. Cutler, 518 F.3d 580, 583 (8th Cir. 2008).

[87] Nader v. General Motors Corp., 255 N.E.2d 765, 767 (N.Y. 1970).

[88] Dietemann v. Time, Inc., 449 F.2d 245, 245 (9th Cir. 1971).

disclosure of private facts.[89] In *Shulman v. GWP*, the plaintiff brought both claims.[90] The final three engaged a reputational interest. In *Time v. Hill* the plaintiff claimed false light,[91] while *Hustler v. Falwell* and *Pavesich v. New England Life Insurance* involved appropriation.[92]

Moreover, among the four cases in which the plaintiff won on at least one claim, three related to intrusion and one to appropriation. None, in other words, involved public disclosure of private facts or false light. While courts have traditionally had difficulty measuring harms to privacy interests,[93] they may have less difficulty with harms to one's reputational interests. While such harms are external to privacy, they are all still related to personal information, and thus may feel "privacy-like."

A second way in which these landmark cases are consistent with this classification into true privacy and reputational interests is that libel and slander appear as additional claims only in cases of the latter, where the privacy torts at issue are either false light or appropriation.[94] This is exactly what we would expect given the discussion in the last Subpart. Like false light and appropriation, the interests protected under libel and slander are reputational, and not truly privacy-based. We would therefore expect that they type of circumstance giving rise a false light or appropriation claim might also give rise to a libel or slander claim.

C. STATUTORY PRIVACY CASES

We can also apply this two-fold classification to help clarify landmark statutory privacy cases. In *Robins v. Spokeo*, Robins brought a Fair Credit Reporting Act[95] action against Spokeo claiming that by running a website that collected public information about people and offering them to "purchase" their own profile, Spokeo had failed in its obligation to take reasonable efforts to ensure the accuracy of such information.[96] In *United States v. Spokeo*, the Federal Trade Commission used its authority under the Fair Credit Reporting Act to

[89] Sidis v. F-R Publishing Corp., 113 F.2d 806, 807 (2d 1940), *cert. denied*, 311 U.S. 711 (1940).

[90] Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 475 (Cal. 1998).

[91] Time, Inc. v. Hill, 385 U.S. 374, 376–77 (1967).

[92] Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 48 (1988); Pavesich v. New England Life Ins. Co., 50 S.E. 68, 69 (Ga. 1905).

[93] *See supra* note 2 and accompanying text.

[94] *Pavesich*, 50 S.E. at 69; *Hustler Magazine*, 485 U.S. at 48.

[95] 15 U.S.C. §§ 1681–1681x (2012).

[96] Robins v. Spokeo, Inc., 742 F.3d 409, 413–14 (9th Cir. 2014); *see also* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545–48 (2016) (vacating and remanding, and holding that the Ninth Circuit failed to fully consider injury-in-fact requirements when determining that the injury suffered is particularized but not considering whether it is also concrete); Robins v. Spokeo, Inc., 867 F.3d 1108, 1108 (9th Cir. 2017) (holding that harm suffered by a violation of the FCRA is an injury sufficiently concrete to confer a plaintiff standing).

bring a substantially similar action against the website.[97] Note that the central issue in Spokeo was not the *existence* of the profiles, but rather the accuracy of the information they contained. In the context of our model, this Spokeo is a case about a shift the man of someone's beliefs, not about its standard deviation. Even though the claims in *Robins v. Spokeo* and *United States v. Spokeo* were brought under the Fair Credit Reporting Act, the issues raised are intimately related to false light and appropriation. They respond to reputational interests, rather than to privacy interests.

Florida Star v. B.J.F.[98] and *Bartnicki v. Vopper*,[99] on the other hand, deal with a privacy interest. *Florida Star* dealt with a state statute prohibiting the publication of a sexual assault victim's name in instruments of mass communications.[100] A local newspaper in Jacksonville, Florida—*The Florida Star*—successfully challenged the constitutionality of the statute under the First Amendment.[101] Bartinicki, for its party, involved Title 3 of the Wiretap Act, which imposes liability on anyone who discloses information obtained in violation of the statute. Applying strict scrutiny, the Court ruled that the application of the provision violated the First Amendment. In both cases, what was at stake was the ability of a third party to obtain true information about the plaintiff.

Florida Star and *Bartnicki* are perfect examples of the importance of distinguishing between reputational interests and privacy interests. In *Florida Star*, the majority reasoned that it would be perverse for defamatory falsehoods to have more protection under the First Amendment than truthful publications. In so doing, it overlooked the fact that truthful information is precisely the type of information that is harmful to one's privacy. Because of this, in an action based on a harm to one's privacy interests, the truthfulness of the information cannot be a mitigating factor. Similarly, in *Bartnicki*, Stevens's opinion is based on the idea that, since truthful information is involved, the speech warrants a high degree of protection under the First Amendment. The statute involved was content-neutral—it did not relate to a specific conduct like the statute in *Florida Star* did—so an intermediate standard of scrutiny should have been applied, but the content-neutrality consideration was

[97] United States v. Spokeo Inc., No. 12CV05001 (MMM), 2012 WL 3862431 (C.D. Cal. June 19, 2012).

[98] Florida Star v. B.J.F., 491 U.S. 524 (1989).

[99] Bartnicki v. Vopper, 532 U.S. 514 (2001).

[100] *Florida Star*, 491 U.S. at 524 (holding that if a news organization lawfully obtains truthful information, the First Amendment bans prohibiting publication—unless a strict scrutiny standard is met).

[101] *Id.*

overruled by the truthful information consideration. In such way, the opinion falls into the same pitfall that the Court fell into twelve years earlier in *Florida Star*.[102]

New York Times v. NASA illustrates a similar point. *The New York Times* presented a Freedom of Information Act ("FOIA") request to NASA asking for information related to an accident. *The New York Times* requested both a transcript related to the accident and knowledge of what was recovered after the fact.[103] The court ruled that NASA was not required to submit the information due to exemption 6 of FOIA[104]—the privacy interest of the astronauts' family members had to be weighed against the public interest. While the default under FOIA is one of disclosure, this default is reversed when privacy interests are strong and the public interest is weak.[105] The case presents a familiar tradeoff between a (in this case strong, according the court) privacy interest and a (in this case weak, according to the court) public interest in the information. It also has echoes of *Shulman* on the question of balancing a privacy interest with what might be considered valuable information.[106]

[102] The purpose of this discussion is to point out the flaw—in both cases—in the court's reasoning regarding the privacy implications of truthful statements. While we are not taking a position on the desirability of granting First Amendment protection to the speech involved or on whether such tradeoff between free expression and privacy was appropriate, such tradeoff should be identified and make explicit regardless of the outcome.

[103] New York Times v. NASA, 852 F.2d 602 (D.C. Cir. 1988).

[104] The exemption provides that agencies should not disclose "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6) (1988).

[105] *See New York Times*, 852 F.2d at 630–32; *see also supra* note 2 (arguing that exemption 6 applies a stricter standard than exemption 7.C for the balancing process).

[106] *See* Shulman v. Grp. W. Prods., Inc., 955 P.2d 469 (Cal. 1998). Like in *New York Times*, the circumstances in *Shulman* began with an accident, this time a car accident. The rescue helicopter that responded to the accident was accompanied by both a video camera operator and a nurse wearing a microphone, resulting in both audio and video recordings of the plaintiffs, certain individuals who were involved in the accident and were rescued. These recordings were then edited and used on Television. The plaintiffs brought two causes of action one based on public disclosure of private facts, and one based on invasion of privacy by intrusion. The California Supreme Court ruled that because freedom of the press protects journalists publishing private facts when the material is newsworthy and of legitimate public concern, summary judgment in favor of the defendants was proper on the first claim. At the same time, it held that the defendants had no constitutional privilege so to intrude on plaintiffs' seclusion and private communications," Shulman v. Grp. W. Prods., Inc. because of the method used to obtain the recordings.

Table 2 shows how these cases fit in the aforementioned scheme.

	Claim	**Outcome**	**Interest**
New York Times v. NASA (1988)	PDPF	Won	Privacy
Florida Star v. B.J.F. (1989)	PDPF	Lost	Privacy
Bartnicki v. Vopper (2001)	Intrusion, PDPF	Lost both	Privacy
United States v. Spokeo (2012)	False light, Appropriation	Lost	Reputation
Robins v. Spokeo (2016)	False light, Appropriation	Lost	Reputation

Table 2. Landmark statutory privacy cases according to their protected interests

In these statutory cases, the divergence of interests mentioned above can be seen as clearly. The first three cases fall squarely under a privacy interest, while the two cases involving Spokeo claim the two aspects of the privacy tort that we identified as referring to a reputational harm. This is unlikely to be a coincidence.

D. Normative Implications of the Model's Distinction

The distinction between true privacy interests and reputational ones is not purely theoretical. While both can be protected by the same common law means, understanding the distinction between the two interests is the first step to more adequately addressing them, and to a deeper understanding of the policy arguments related to their protection.

Take, for example, the economic argument that if someone is portrayed under a false light, what will help the person is more information, not less.[107] Privacy is ineffective, the argument goes, at solving problems of false impressions. We can use this model to characterize this argument as follows: suppose that, because of false light, Ben has a mistaken impression of Abby's type: the mean of his posterior distribution is too low. The solution is for him to learn *even more* about her. As he does so, the false light will gradually have less and less of an effect on his posterior, until it is entirely overwhelmed by the truth. On the surface, this seems like a puzzle. After all, we generally think that the reason we have privacy is not a concern that Ben will get the wrong idea about Abby; the reason we have privacy is that without it, Ben will progressively come to have the *right* idea about Abby.

[107] Posner, *supra* 6, at 408.

This model of privacy helps see that the reason for the (limited) success of this critique is that the pro-privacy argument would, in fact, make little sense if the tort of false light protected a true privacy interest. However, once we recognize that it is actually protecting a reputational interest using a privacy rule, the critique becomes easier to address. The reason for protecting this interest with a privacy rule is pragmatic: people have limited time and attention. They have neither the time nor the inclination to acquire and process infinite amounts of information. Rectification—the dissemination of truthful information ex post—as an alternative means of protecting this reputational interest, might therefore be ineffective. A rectification may not reach all recipients of the initial (false) information, or these recipients may simply not bother to fully process the new information.[108]

The proposed framework also has implications for the relationship between privacy and the First Amendment, a relationship that has long troubled the Supreme Court.[109] The leading case, *Hustler Magazine v. Falwell*, in which the Court ruled that a public figure does not have redress for emotional distress caused by a caricature that a reasonable person would not interpret as factual,[110] illustrates this idea particularly well. Even though ruling in *Hustler*'s favor, the Court's holding in *Falwell* rests partly on the argument that false or misleading statements, such as the caricatures published by *Hustler*, are valueless, and sometimes even harmful, in the market of ideas.[111] In other words, the Court drew a distinction between true facts (covered by the first two privacy torts), which implicate First Amendment protection, and misleading facts (covered by the third privacy tort), which do not.[112] This traces back to the distinction between privacy's two protected interests.

The distinction between these two interests has profound implications for the relationship between privacy and the First Amendment. Specifically, it gives us a framework for analyzing the extent to which a piece of information's truth can be used as a First Amendment defense for disclosures that could be privacy invasive. Privacy-based limitations to the disclosure of truthful information are difficult to sustain under the First Amendment. Consequently, when the First

[108] JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000); Lawrence Lessig, *Privacy and Attention Span*, 89 GEO. L.J. 2063, 2063–64 (2001).

[109] Florida Star v. B.J.F., 491 U.S. 524, 530–33 (1989); Frisby v. Schultz, 487 U.S. 474, 484–88 (1988). *See* Post, *Constitutional Concepts*, *supra* note 75, at 615.

[110] Hustler Magazine v. Falwell, 485 U.S. 46 (1988).

[111] Post, *Constitutional* Concepts, *supra* note 75, at 613 (citing Hustler Magazine v. Falwell, 485 U.S. 46, 55 (1988)).

[112] The fourth tort, which hinges on the use of one's image, does not relate to facts at all, neither collaborating nor harming the marketplace of ideas.

Amendment is involved, the torts referring to the true privacy interest should be given more prominence than those that refer to a reputational interest.

In *Falwell*, the court decided that truthful information is entitled to more First Amendment protection than misleading information.[113] Nevertheless, as a political community, we might want to give a higher level of protection to plaintiffs who have experienced a privacy harm due to the dissemination of *truthful* information. The Court addressed this issue in *Florida Star v. B.J.F.*, where the newspaper, *The Florida Star*, revealed the name of a sexual assault victim, in violation of State law. The Court ruled that it would be a perverse result if the First Amendment protected a truthful publication less than it protects defamatory falsehood.[114] This ignores the degree to which the dissemination of true information can be privacy invasive, and hence how harmful it can be.[115] Our framework can help clarify this. The dividing line for the relationship between privacy and the First Amendment protected speech should be determined not only by whether the information is truthful, but rather by how much harm the victim would sustain relative to the social benefit of disclosing this information. In *Florida Star*, for example, the harm to the victim might have been quite substantial, while the social benefits of knowing her name might have been small.

The role of truth in information leads to our model's third implication. Analyzing privacy claims in terms of the truth (or lack thereof) of the information is justified only in cases where what is at stake is a reputational interest, and not when it is a privacy interest. To dismiss a privacy claim because the statement at issue is false when the protected interest is a reputational one (such as false light) would be a mistake. The core of any reputational harm is that the plaintiff's reputation has been wrongfully degraded in the eyes of a third party. The harm—the wrongful degradation of the victim's reputation—is inflicted by the falseness of the assertion. The truthfulness of the statements in question therefore lie at the core of reputational protection.

On the other hand, truthfulness cannot be a valid defense when privacy is the protected interest. As we have shown, the central feature of protecting an individual's privacy interest is to measure how she is harmed by when another learns more about her. If someone learns

[113] *Falwell*, 485 U.S. at 56 ("we conclude that public figures and public officials may not recover for the tort of intentional infliction of emotional distress by reason of publications such as the one here at issue without showing an addition that the publication contains a false statement of fact which was made with 'actual malice'") *Id.*

[114] *Florida Star*, 491 U.S. at 540–41; *see also supra* Subpart B.

[115] In this case in particular, it undervalued how harmful it was for sexual assault victims to have their names disclosed publicly.

something *false* about her, this might harm her reputation—as discussed above—but it does not affect her privacy. In other words, the truthfulness of the information in question *increases* the harm to the victim. Privacy harms refer to a protection over certain aspects of our private life, while reputational harms refer to a protection over undeserved attacks to one's public persona. True information, therefore, is especially harmful for privacy interests, while false information is harmful for reputational interests.

This explains why an effective rectification can address a reputational harm, but cannot address a privacy harm. Provided it can overcome the fact that people have limited time and attention, new, truthful, information can often dilute or nullify the harmful effect of false information.[116] When the harm is to a privacy interest, in contrast, more truthful information can never help. Privacy harms can at best be reduced with the passage of time and people's faulty memories—if not recorded online.[117] If Cameron had evidence that the embarrassing event of which he was accused had not taken place, he could at least partially remedy his reputation by presenting it to the public. Assuming that this evidence was seen as credible, the harm to his reputation would have been substantially mitigated. If, on the other hand, what had been disclosed was a true and embarrassing fact about his preferences, so that people's probability distribution about him would be narrowed, more information would only have produced more harm.

Finally, our framework suggests that a revaluation of the harm standards used in adjudicating privacy and related torts is in order. The main difference between the privacy tort and other related torts (such as libel, slander, and intentional infliction of emotional distress), is that the privacy tort does not require the plaintiff to prove a separate harm. Instead, the loss of privacy is itself sufficient.[118] This is, deep down, an evidentiary difference. In cases involving the privacy tort, courts can assume that a privacy harm is already present. In contrast, a plaintiff must prove harm in a claim of intentional infliction of emotional distress, and must prove reputational harm in an action for libel or slander.

Our model, along with the foregoing analysis, makes clear that this lower evidentiary standard should apply only to claims based on a true

[116] *See* ROSEN, *supra* note 108.

[117] *See* VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2009) (arguing that there should be a time limit for online information, emulating people's memories, to protect people's privacy online).

[118] RESTATEMENT (SECOND) OF TORTS § 652H (AM. LAW. INST. 1977); *see also* Socialist Workers Party v. Attorney Gen. of the U.S., 642 F. Supp. 1357, 1421 (S.D.N.Y. 1986); Manville v. Borg-Warner Corp., 418 F.2d 434, 437 (10th Cir. 1969); Cason v. Baskin, 159 So.2d 635, 340 (Fla. 1947) (cited in Post, *Constitutional Concepts*, *supra* note 75, at 624.)

privacy interest, not to reputational interests protected by privacy rules. In other words, only intrusion upon seclusion and public disclosure of private facts should be subject to this lower evidentiary burden. Since false light and appropriation do not imply by themselves a harm to the victim's true privacy interest, some indication of diminished reputation—similarly to that required for libel and slander—should be required for them.

IV. Fourth Amendment Doctrinal Consequences

This model can also help to clarify an important area of constitutional law: the much criticized Fourth Amendment third party doctrine. The key problems with this doctrine stem from the fact that it rests on an unsatisfying conception of privacy that views privacy as secrecy, and it does so in a dichotomous way. The considerations set above are also relevant for a controversial case currently before the Supreme Court: *Carpenter v. United States*.

A. The Third Party Doctrine: Law and Existing Critiques

1. Judicial Critiques

In *Katz v. United States*, the Supreme Court held that a search or seizure violates the Fourth Amendment if conducted against reasonable expectations of privacy.[119] When a person makes a call from a telephone booth with the door shut, the court held, that person is entitled to such expectation.[120] As a result, the government must procure a warrant to record such a conversation.[121] The third party doctrine is used to define the scope of a reasonable expectation of privacy under the Fourth Amendment.[122] It establishes that, when someone voluntarily discloses information to a third party, she has no reasonable expectation of privacy over that information (*United States v. Miller*, *Smith v. Maryland*)—and thus the government can obtain and use that that information without a warrant.[123]

[119] Katz v. United States, 389 U.S. 347, 350–53 (1967).

[120] *Id.*

[121] *Id.*

[122] The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ." U.S. CONST., amend. IV.

[123] United States v. Miller, 425 U.S. 435, 433 (1976); Smith v. Maryland, 442 U.S. 735, 744 (1979). In *Miller*,

> [t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the

The Supreme Court first used the third party doctrine to define reasonable expectations of privacy in *Smith v. Maryland*, where it held that using pen registers to obtain what numbers a person has dialed is not a search, and therefore does not require a warrant.[124] The line of reasoning is as follows: the Court had held before that people have no reasonable expectation of privacy with respect to information that is voluntarily conveyed to others.[125] In other words, when *Smith* was decided, if Abby had talked to Ben and he had repeated what Abby had said to the police (she was "betrayed by her confidant"), there would have been no Fourth Amendment violation.[126] The Court had determined in *On Lee v. United States* and *Lopez v. United States*, that the presence of electronic recording did not change this Fourth Amendment analysis.[127] Rather than repeating to the police what Abby said, the argument goes, Ben could have recorded her and handed the recording to the police. Moreover, the Court had held in *United States v. White* that the reasonable expectations of privacy rule and the protections afforded by *Katz* do not alter this conclusion.[128] As a result, Smith had no Fourth Amendment protection because he had "voluntarily conveyed numerical information to the telephone company."[129]

The Court had used an equivalent criterion before in *Miller* for bank records. It held that people have no expectation of privacy over bank records because these are voluntarily shared with the bank.[130] *Smith* consolidated the principle, known as the third party doctrine, that information shared with third parties has no protection under the Fourth Amendment.

Many have criticized the Court's reasoning in *Smith*. Some lower courts have evidenced discomfort with it even when considering

> assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

425 U.S. at 443 (citation omitted). In *Smith*, "this Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." 442 U.S. at 743–44.

[124] *Smith*, 442 U.S. at 742.

[125] *Id.* at 743 ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

[126] *Id.*

[127] On Lee v. United States, 343 U.S. 747, 753 (1952); Lopez v. United States, 373 U.S. 427, 440 (1963).

[128] United States v. White, 401 U.S. 745, 752–53 (1971); *see also* Katz v. United States, 389 U.S. 347, 351–52 (1967) (citation omitted) ("[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

[129] Smith v. Maryland, 442 U.S. 735, 744 (1979).

[130] United States v. Miller, 425 U.S. 435, 440–42 (1976).

themselves bound by it.[131] In his dissent in *White*, Justice Harlan argued that to think that every time one talks with a friend one is assuming the risk of being recorded is to misunderstand the set of behaviors that constitute normal social interactions. While the possibility of being betrayed to the police is a part or normal social interactions, being recorded is not.[132] Under Harlan's view, the scope of normal social interactions should be central to the third party doctrine, just as it is to the concept of a reasonable expectation of privacy more broadly.

Similarly, in *Florida v. Riley*, where the police observed a marijuana plantation from the air, O'Connor's concurring opinion mirrors Harlan's dissent in *White* in defining reasonable expectations of privacy. While not primarily concerned with the third party doctrine, her opinion is nevertheless informative. In it, she argued that what is relevant for privacy is not whether the helicopter that was used to fly over Riley's property was legally entitled to fly at the height at which it did (as it was in the majority opinion), but rather that objects flying at such height are "a sufficiently routine part of modern life [so] that it is unreasonable for persons on the ground to expect that their curtilage will not be observed from the air at that altitude."[133] By leaving something exposed to objects that routinely fly at that height, Riley ran the risk that they could be viewed by third parties.

The majority opinion in *Kyllo v. United States* saw the issue in the same way. There, the case centered on the use of thermal imaging to detect heat coming from inside a person's home. The Court stated that, if the thermal imaging technology at issue had been in common use in society, the information collection would have fallen outside of one's expectations of privacy. Because it was not, the use of thermal imaging was held to be illegal.[134] This is in tension with the majority's reasoning in *Riley*. Under the reasoning in *Riley*, one should conclude that *Kyllo* would have no expectation of privacy as long as the use of thermal

[131] *See* United States v. Davis, 785 F.3d 498, 519–21 (11th Cir. 2015) (en banc) (Pryor, J., concurring) ("If the third-party doctrine results in an unacceptable 'slippery slope,' the Supreme Court can tell us as much"); *id.* at 525 (Rosenbaum, J., concurring):

> [U]nless a person is willing to live 'off the grid,' it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life. And the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling.

United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) (en banc) ("The Supreme Court may in the future limit, or even eliminate, the third-party doctrine."); *id.* (Stranch, J., concurring) ("[W]e need to develop a new test to determine when a warrant may be necessary under these or comparable circumstances.").

[132] *White*, 401 U.S. at 776–77 (Harlan, J., dissent).

[133] Florida v. Riley, 488 U.S. 445, 453 (1989) (O'Connor, J., concurring).

[134] Kyllo v. United States, 533 U.S. 27, 40 (2001).

imaging is legal. The majority opinion in *Dow Chemical v. United States*, in which the Court asked whether the aerial camera used was accessible to the general population, also followed this line of reasoning.[135]

2. *Doctrinal Critiques and Proposals*

We are hardly the first to argue that the third party doctrine is deeply flawed. In its current form, the third party doctrine is almost certain to lead to a progressive erosion of privacy: as technologies advance and become ever more widespread, and as more means of communication require an intermediary, more "third parties" are involved in people's communications.[136] It would be wrong to argue that, simply because the standard means of communication have mutated into more convenient ones, people should progressively have less privacy.[137] Nevertheless, this is exactly what the third party doctrine implies.[138] This runs counter to the whole scholarly privacy conversation, which centers on how to maintain people's privacy with the advent of technologies that facilitate the gathering, storing and disseminating personal information.[139]

The artificiality of creating a dichotomy between keeping something "private" and sharing it with one or a few particular individuals is especially evident in a networked world, where being part of society necessarily means selectively sharing information. This idea is captured by Marshall's dissent in *Smith*, which emphasizes the petitioner's lack of choice in communicating through a means that involves a third party intermediary.

The third party doctrine is built on the argument that, when people share information with another party, they willingly assume a risk of leakage.[140] But this assumption of risk argument implies the existence of

[135] Dow Chemical Co. v. United States, 476 U.S. 227, 234–39 (1986).

[136] Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1225–26 (2016).

[137] Kerr, for example, believes that we should use "equilibrium-adjustment," and apply the Fourth Amendment to situation in which technological changes are involved in a way that we maintain the level of constitutional protection constant. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) [hereinafter Kerr, *An Equilibrium-Adjustment*]; *see also* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285 (2015) [hereinafter Kerr, *The Fourth Amendment*].

[138] Kerr, *An Equilibrium-Adjustment*, *supra* note 137, at 482-93 (introducing the theory of equilibrium-adjustment); Kerr, *The Fourth Amendment*, *supra* note 137 (showing how equilibrium-adjustment responds to the issues of internet surveillance).

[139] *See* Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119 (2002) (arguing that the Supreme Court has devaluated Fourth Amendment privacy). Someone could counter-argue that technology brings both privacy-invading and privacy-enhancing possibilities, but our experience shows that the former tend to outnumber and outpower the latter.

[140] *See supra* text accompanying notes 83-89.

an unexercised choice to use other means, and members of our society do not have a real choice to use many of the means of communication that are rendered non-private by the third party doctrine. In this regard, Marshall objected to the notion that "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."[141]

While taking the doctrines in the right direction, Marshall's position is insufficient. The dissent does not propose a resolution to the question of what constitutes a choice. Are we choosing to put our information at risk by sending a non-encrypted email? What about by sending an e-mail at all, as opposed to a letter through (arguably more secure) airmail?

To solve the problems created by the influence of technology in the third party doctrine, Jack Balkin introduces the concept of "information fiduciaries."[142] "An information fiduciary is a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship."[143] In the digital age, Balkin explains, we have no choice but to trust our information to online service providers and, when we do, we should expect such information to be treated according to a relationship of trust.[144] This alters our reasonable expectation of privacy as it places information intermediaries alongside lawyers and doctors, excepted from the assumption of the third party doctrine that the information is publicized when it is shared.[145] This approach is compatible with Marshall's focus on whether we have an option to disclose the information to the third party. It is also helpful to keep the "equilibrium" of privacy and the Fourth Amendment with the emergence of new technologies,[146] and to develop a more robust set of exceptions in which the third party doctrine is not applied, thereby avoiding some of its most objectionable results. The existence of information intermediaries, which could be turned into information fiduciaries, increases the number of

[141] Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

[142] Balkin, *supra* note 136, at 1205–09; *see also* Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016) (proposing that privacy law should further rely on trust in the use of information, similarly to fiduciary law).

[143] Balkin, *supra* note 136, at 1209.

[144] Balkin, *supra* note 136, at 1230–31. ("We have a reasonable expectation, in other words, that people and organizations who owe duties of trust and confidence to us will not betray us.").

[145] Balkin, *supra* note 136, at 1230–31 ("We provide lots of information about ourselves—some of it quite sensitive—to people and organizations who owe us fiduciary duties or duties of confidentiality. And when we provide this information, we have, and should have, a reasonable expectation that they will respect our privacy."); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 611 (2015) (arguing that not only the third party doctrine is in need of modification, but the whole Fourth Amendment doctrine's approach to general information is).

[146] *See* Kerr, *An Equilibrium-Adjustment*, *supra* note 121; Kerr, *The Fourth Amendment*, *supra* note 121.

cases in which the third party doctrine generates undesirable outcomes.[147] Today, an immense amount of personal information is collected and stored by private third parties. Much of this information then flows to the government, who can create detailed records of individuals that seem to stand at odds with the Fourth Amendment.[148]

Unlike the proponents of the information fiduciaries theory, we do not seek to expand the exceptions to the current third party doctrine. Rather, in the next Subpart, we argue for a new approach to privacy under the Fourth Amendment.

B. Implications of Our Model

1. A Way Forward

In line with the information fiduciaries idea, our model shows that the core problem with the third party doctrine is that it interprets privacy as secrecy, and it does so in a dichotomous way.[149] Sherry Colb has demonstrated that the post-*Katz* Fourth Amendment decisions have narrowed the scope of reasonable expectations of privacy by treating "exposure to a limited audience as morally equivalent to exposure to the whole world."[150] This can be seen, for example, in cases defining Fourth Amendment protection over garbage. In *California v. Greenwood*, where the Court asked whether examining garbage left on the street in a closed opaque bag is a Fourth Amendment search,[151] one of the key arguments was that the individual deliberately handed the garbage to a third person: the garbage collector, who could have potentially opened the bag and exposed its contents when moving it to the truck.[152]

Our model shows why this equivalence is misguided. What is disclosed to one person cannot be treated as though it has been *publicly* disclosed (and therefore unconcealed), rendering further disclosure

[147] New technologies sometimes impose new problems for the law. They blur distinctions that were formerly clear, they introduce new slippery slopes, and they demand analogies that are unobvious to interpreters. But, often, new technologies make salient problems that the law already had. They bring counterexamples that were nonexistent and take contradictions, assumptions and circularities to surface.

[148] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084–86 (2002). *But see generally* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2013) (denying standing because the injury is not "certainly impeding").

[149] *See* Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 657–59 (2013) (arguing that Fourth Amendment doctrine is disconnected from society's conception of privacy because courts rely on binary distinctions, and reexamining the meaning of the Fourth Amendment's "reasonable expectation of privacy" using the theory of contextual integrity).

[150] Colb, *supra* note 139, at 122 (also showing that this followed a prior analytical move of equating risk of exposure with an invitation to such exposure).

[151] *See generally* California v. Greenwood, 486 U.S. 35 (1988).

[152] Colb, *supra* note 139, at 153–55.

harmless. Absolute secrecy is a narrow and hardly defensible conception of privacy that runs contrary to our intuitions about privacy. To use a popular example, describing a man on a deserted island (who shares his information with no one) as a very private man would be meaningless.[153] This conception of privacy has also been met with resistance in privacy scholarship, where most consider it not to be privacy's meaning.[154] This problem is enhanced by the dichotomous view of privacy.[155] Under a more complete conception of privacy, it becomes clear that the current third party doctrine leads to counterintuitive and objectionable results.[156]

Carpenter is a perfect illustration of how the model above helps identify the problems with this doctrine. During a criminal investigation, the government procured 152 days of historical cellphone location data from Timothy Carpenter without securing a warrant. It did so based on the Stored Communications Act ("SCA"), which contemplates disclosure orders without need for a probable cause as long as there are "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[157]

Carpenter asked to suppress the records, arguing that the SCA's reasonable grounds standard violates the Fourth Amendment.[158] The district court denied the motion and stated that acquiring cellphone records is not a search, relying on *United States v. Skinner*, which held that no warrant is needed to procure short-term and real-time tracking of suspects' cellphones.[159] The Sixth Circuit, in a three-judge divided panel, affirmed, holding that there is no expectation of privacy, and no Fourth Amendment protection for these location records because they are business records that reveal routing information and not the content

[153] *See* Fried, *supra* note 27.

[154] *See supra* Part I.A; Solove, *supra* note 148.

[155] LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 1391 (2d ed. 1988) (arguing that the tendency of the Supreme Court to treat privacy as a discrete commodity is alarming); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. POL'Y 211, 258 (2005) (arguing that a controlled disclosure to a third party is not equivalent to an indiscriminate disclosure).

[156] Crocker has even argued that the third party doctrine places information privacy into conflict with decisional privacy. As argued for decisional privacy in *Lawrence v. Texas*, privacy protects, and therefore the government cannot interfere with, intimate conducts that take place within interpersonal relationships—thus making clear that privacy does not only protect what we keep to ourselves. Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After* Lawrence, 57 UCLA L. REV. 1, 23–25 (2009). *See generally* Lawrence v. Texas, 539 U.S. 558 (2003) (finding that Petitioners were entitled respect for their private lives).

[157] 18 U.S.C. § 2703(d)(2012).

[158] Brief of Petitioner-Appellant at 36a, Carpenter v. United States, No. 16-402 (Aug. 7, 2017).

[159] Carpenter v. United States, No. 12-20218, 2013 WL 6385838, at *2 (E.D. Mich. Dec. 6, 2013).

of communications.[160] In doing so, the Sixth Circuit relied on *Smith v. Maryland* and the third party doctrine.[161] The Supreme Court heard oral arguments for the case on November 29, 2017.

If the Court were to simply apply the third party doctrine to *Carpenter*, it would hold that he had no reasonable expectation of privacy regarding his geolocation, as he shared it with his telephone provider.[162] This has been the central argument of the U.S. government in its brief and the oral arguments.[163] Our discussion above shows why this conclusion would be mistaken.[164] Sharing his location with his telephone provider (on which he had no choice) does not cause Carpenter the same disutility as sharing it with the entire world—including the U.S. government.

Under our model, revealing information to a party implies a reduction in the standard deviation of his posterior (a privacy loss). The current third party doctrine would use this reduction as a reason for imposing *a further* reduction in standard deviation (this is, there will now be a tightening of *another* individual's distribution) by passing the information along to another party. This is illogical. Abby might tell something to Caroline because her loss in privacy (if any) is compensated by a gain in friendship produced by the disclosure, but this does not imply that Abby is unharmed if the information is given also to Ben.[165]

While this problem is magnified in a networked world, it also occurs with the use of technologies that have existed for some time. For example, consider the release by the news site Gawker of a private recording made

[160] Carpenter v. United States, 819 F.3d 880, 884 (6th Cir. 2015).

[161] *But see id.* at 892–93 (Stranch, C.J., concurring) (arguing that the case, given the quantity of sensitive information procured, raises issues similar to those of *United States v. Jones*, but invoking a good faith exception to the exclusionary rule).

[162] *See infra* note (insert for new Steven Shavell cite).

[163] Brief of Respondent-Appellee at 12–26, Carpenter v. United States, No. 16-402 (Aug. 7, 2017); transcript of oral argument at 41, https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/16-402_6khn.pdf (Deputy Solicitor General arguing that "[companies] make decisions based on their own business needs about what they're going to retain. And when the government comes and asks them to produce it, it is doing the same thing that it did in Smith. It is doing the same thing that it did in Miller. It is asking a business to provide information about the business's own transactions with a customer. And under the third party doctrine, that does not implicate the Fourth Amendment rights of the customer.").

[164] In the oral arguments, the Court discussed the moderating principles we surveyed earlier. For example, Justice Breyer said that "the law is at the moment [that] third-party information is third-party [doctrine], with a few exceptions, but it maybe that here another exception should exist for the reason that the technology, since the time those cases have—has changed dramatically." Transcripts, *supra* note 163, at 65. At the same time, however, the Court recognized the extreme difficulty of line drawing for this issue. Transcripts, *supra* note 163, at 66–73.

[165] This is based, once again, on a linear conception of privacy. A more complex version of the model would include context. We could think of Abby's relationships with different people as different distributions. Such version would make this argument, and thus would reject the viability of the third party doctrine, in a stronger way.

by Terry Gene Bollea (Hulk Hogan) having intercourse with his neighbor. The recording received significant media attention.[166] The jury ruled in favor of Bollea, finding that Gawker breached his privacy (public disclosure of private facts) and awarding him $115 million in damages.[167] Under the logic of the third party doctrine, if it were applied this privacy tort, Bollea would have had no privacy interest in the tape. There was no absolute secrecy because he was, after all, in the company of another person. There was, therefore, at least one other person who was aware of the contents of the recording. This would certainly be an absurd conclusion independently of whether the third party to whom the information is shared is another individual or the government, which shows how the problems of the third party doctrine, while increased by information intermediaries, predate them.

Similarly, the rule would also reach absurd results if applied to information shared with lawyers, priests, doctors or psychologists.[168] These cases could until now be taken as exceptions produced by their fiduciary duties, but new technologies have made ubiquitous those cases in which the third party doctrine would lead to objectionable results.[169] Because the type of communications for which the third party doctrine does not work has changed from being an exception to being the rule, listing exceptions cannot continue to correct for its root problems for much longer.

The information fiduciaries solution would represent enormous progress for current Fourth Amendment law.[170] Like Marshall's options approach, it does not attempt to solve the root problem of the third party doctrine, built on a dichotomous conception of privacy.[171] The solution does not intend do away with the third party doctrine but to limit its application to those entities that are not considered fiduciaries, therefore reducing most of its damage.[172]

[166] Matt Ford, *In First Round with Gawker, Hulk Hogan Prevails*, ATLANTIC (Mar. 19, 2016, 1:20 AM), http://www.theatlantic.com/national/archive/2016/03/gawker-hulk-hogan-verdict/474528/.

[167] *Id.*

[168] Balkin, *supra* note 136.

[169] Balkin, *supra* note 136, at 1231 (noting "that this would not be the end of the third-party doctrine. It would still continue to apply in all cases in which we provide information to someone who is not an information fiduciary. In fact, the concept of information fiduciaries is especially helpful because it gives us an intermediate position between enforcing the third-party doctrine as it currently stands and getting rid of it entirely.").

[170] The idea also addresses problems for privacy in consumer law, such as imposing duties on such fiduciaries while avoiding constitutional challenges based on the First Amendment. *See* Balkin, *supra* note 136, at 1231.

[171] Reducing privacy to a dichotomous is not inherent to the fiduciary solution (or to the options solution) but part of the structure of the third party doctrine. The theory could be more useful to solve problems in Fourth Amendment doctrine if disposed from this dichotomous conception.

[172] Balkin, *supra* note 136, at 1231.

This makes the idea of information fiduciaries implementable, realistic, and helpful. Applying the third party doctrine while accepting the idea of information fiduciaries would have changed the results of *Miller* and *Smith* because there was an intermediary with a relationship of trust involved—the bank and the telephone company, respectively.[173] However, it would also have (mistakenly) led to rule in favor of the government in *United States v. Jones*[174] and *Riley v. California* because there was no information fiduciary involved to introduce an exception to the third party doctrine, and it would have (again mistakenly) not changed the outcome of *White* for the same reason. By creating a set of exceptions, the information fiduciaries proposal helps to alleviate the new problems that new technologies pose for the doctrine. But no solution other than doing away with the third party doctrine altogether can address its root problems: a mistaken assumption of what privacy is and the conditions under which it is appropriate to assume that a person placed a piece of information at risk of public disclosure.

Whereas Fourth Amendment doctrine has defined search, and therefore privacy, in a dichotomous way, our model makes clear that privacy is properly understood as a continuum. On the surface, these two conceptions—dichotomous versus continuous—seem irreconcilable. They are not. By combining this model with some of the most fundamental concepts in the common law tradition, we propose how to address the third party doctrine.

2. *Care and Culpability: Two Instances of Cutoff Rules*

Drawing on our model, we propose an alternative solution. We have already argued that privacy is best viewed as a continuum. We argue that courts should take this into account when determining whether an action qualifies as a search for the purposes of the Fourth Amendment. We make this argument in three steps. First, we show that the law is already equipped to deal with the problem of converting a continuum into a yes/no dichotomy by pointing to both substantive criminal law and tort law. We then draw on concepts borrowed from tort law, and show that the current third party doctrine is the privacy equivalent of a strict liability rule. We then argue that this rule is inappropriate, and that a negligence style standard is more appropriate.

[173] This could, and perhaps should, have been the result for Miller even without the idea of information fiduciaries, given that the Bank Secrecy Act required banks to keep such records confidential. 12 U.S.C. § 1829b(d) (2012). The Court dismissed the importance of this rule under the argument that Miller could not assert ownership over the records, which were owned by the bank. United States v. Miller, 425 U.S. 435, 440–42 (1976).

[174] United States v. Jones, 565 U.S. 400, 413–21 (2012).

The law is full of instances in which a continuous variable is converted into a dichotomous outcome. In criminal law, for example, Section 2.02 of the Model Penal Code defines the different levels of culpability as: purposely, knowingly, recklessly, and negligently.[175] Each of these represents a cutoff point. The law defines crimes as requiring a level of culpability *at least as great* as the level specified in the statute. In fact, in section 2.02(5), the Code acknowledges the continuous nature of culpability by establishing a hierarchy between levels and stating that each of them is encompassed by the others.[176] If one can use cutoff points along a continuum to define culpability for substantive criminal law, there is no reason why one cannot do the same for criminal procedure.

We find a similar set of cutoffs along a continuum in the tort law context. This is a particularly appropriate parallel to the Fourth Amendment context since, at the time of a search, one is not interested in assigning blame. In the tort context, a finding of negligence implies a lower standard of culpability than a finding of recklessness for it. As a result, behavior that might be held to be tortious under a negligence standard might not be sufficient to meet a recklessness standard. At the extreme lies a strict liability standard, where only cause, and no subjective element, is required for culpability. While under recklessness or negligence one can perform the activity in question while insulating oneself from potential liability (by doing so with care), under a strict liability standard, there is nothing one can do other than abstaining from the activity altogether.

3. *The Third Party Doctrine as Strict Liability*

The current third party doctrine is the equivalent of strict liability in privacy law.[177] There is no action that Abby can take, other than not verbalizing the information, to keep it within the scope of the Fourth Amendment's protections. This is roughly equivalent to saying that there is nothing that Abby can do to keep herself from being liable for the

[175] MODEL PENAL CODE § 2.02(2)(a)–(d).

[176]

> Substitutes for Negligence, Recklessness and Knowledge. When the law provides that negligence suffices to establish an element of an offense, such element also is established if a person acts purposely, knowingly or recklessly. When recklessness suffices to establish an element, such element also is established if a person acts purposely or knowingly. When acting knowingly suffices to establish an element, such element also is established if a person acts purposely.

MODEL PENAL CODE § 2.02(5).

[177] *Cf.* Colb, *supra* note 139, at 144–46 (advancing the similar argument that the concept of "knowing exposure" is equivalent to search consent and this equivalence make them analogous to the often criticized strict liability criminal offenses, albeit lacking their public welfare justifying rationale).

disclosure.[178] In the same way that a factory that builds widgets under a strict liability rule can eliminate potential liability only by abstaining from production altogether, Abby can only ensure that her privacy is protected under the Fourth Amendment by abstaining from any disclosure. In other words, just as there is no level of care that is sufficient to protect a potential tortfeasor from liability under a strict liability rule, there is *no* series of steps Abby can take, short of staying silent, to ensure that the content of her disclosure cannot be accessed by the police. Yet, while there are good reasons to have strict liability in some tort contexts, these reasons do not carry over to the Fourth Amendment context.

4. Strict Liability and Culpability Appropriateness

The most common places where one can find liability in tort law are products liability and liability for inherently dangerous activities. While the argument for the former is economic in nature, the argument for the latter tends to be principle-driven. We argue that the both arguments are inapposite in the Fourth Amendment context.

From an efficiency perspective, strict liability is efficient when the probability of the accident can only be controlled by the potential tortfeasor and this probability is determined by both the tortfeasor's level of care and activity. More specifically, strict liability is efficient when one party can most efficiently bear the risk of harm.[179] A key aspect of the economic approach to tort law is its focus on dynamic efficiency: the goal is less to ensure an efficient outcome ex post than it is to create incentives for efficient behavior ex ante.

Using this framework, it is difficult to see how a strict liability rule is compatible with the Fourth Amendment. To begin with, there is no reasonable analogy between product liability—a commercial context—and a social conversation between two humans.

Moreover, while there is undoubtedly a worthy social goal involved—solving crimes—the third party doctrine goes about advancing this goal only from an ex post perspective. Only *after* the information has been transmitted from Abby to Ben does the third party doctrine come into play, and ensures an ex post transfer of that information on to the police. From an ex ante perspective, however, the third party doctrine does nothing to create efficient incentives to disclose information in the first place. On the contrary, it creates incentives for individuals to guard

[178] *See* Ignacio Cofone, *The Dynamic Effect of Information Privacy Law*, 18 MINN. J.L. SCI. & TECH 517, 534–542 (2017) (explaining that disclosure can be seen as production of personal information).

[179] STEVEN SHAVELL, ECONOMIC ANALYSIS OF ACCIDENT LAW 5–46 (2007).

their information as closely as possible. While this may make little difference to the police, the collateral social consequences are troubling.

In fact, the collateral social consequences of the third party doctrine are similar in many respects to the consequences of eschewing informational privacy altogether. There is a consensus among scholars that privacy, in general, encourages other values such as autonomy, personhood, and free speech,[180] so much so that most privacy considerations discussed in Part I, either explicitly or implicitly, rest on this argument. The logic behind this is simple: if, after Abby discloses something to Ben, she has no guarantee that this information won't be passed on to someone else, she will simply talk to Ben less. From Abby's perspective, this risk—which, in the context of the third party doctrine, includes the risk that the information will be passed on to law enforcement—represents a cost of disclosure. If the law is such that turns every member of society into a potential police informant, Abby now lives in a society that we would consider undesirable.

We recognize that the third party doctrine is not solely a question of efficiency. Similarly, tort law also uses strict liability for inherently dangerous activities or things, such as fireworks or dangerous animals.[181] In such cases, there is generally an underlying sense that what the tortfeasor has done is morally suspect, though not necessarily wrongful. The moral intuition behind strict liability in such cases follows from this sense that the tortfeasor had no business engaging in these activities to begin with.

This argument for strict liability is even less appropriate in the Fourth Amendment context. There is nothing morally questionable about most interpersonal communications. And while there may be a vague sense that anyone under investigation by the police is tarred with a veneer of criminality, this intuition is at odds with the presumption of innocence, which is the bedrock principle of the criminal justice system.

[180] *See supra* Part I.A.

[181] According to the Second Restatement of Torts,

> (1) Once who carries on an abnormally dangerous activity is subject to liability for harm to the person, land or chattels of another resulting from the activity, although he has exercised the utmost care to prevent the harm. (2) This strict liability is limited to the kind of harm, the possibility of which makes the activity abnormally dangerous.

RESTATEMENT (SECOND) OF TORTS § 519 (2nd 1979);

> (1) A possessor of a wild animal is subject to liability to another for harm done by the animal to the other, his person, land or chattels, although the possessor has exercised the utmost care to confine the animal, or otherwise prevent it from doing harm. (2) This liability is limited to harm that results from a dangerous propensity that is characteristic of wild animals of the particular class, or of which the possessor knows or has reason to know.

RESTATEMENT (SECOND) OF TORTS § 507 (2nd 1979).

As Cynthia Lee has pointed out, the Supreme Court has long characterized the Fourth Amendment as operating under a reasonableness analysis:

> The Supreme Court's definition of a "search" within the meaning of the Fourth Amendment turns on whether the defendant's expectation of privacy was *reasonable*. The Court's definition of a "seizure" of the person turns on whether a *reasonable* person in the defendant's shoes would have felt free to leave or terminate the encounter with the police officer. Probable cause to search is defined as *reasonable* grounds to believe that evidence of a crime will be found in the place to be searched. Officers can conduct a *Terry* stop upon *reasonable* suspicion of criminal activity and can do a *Terry* frisk of the person if they have *reasonable* suspicion that the suspect is armed and dangerous. And, increasingly, the validity of a search turns on whether the reviewing court believes the search was reasonable.[182]

This should be unsurprising, since the text of the Fourth Amendment refers to *unreasonable* searches and seizures. In the words of the Court itself in *Riley*, "As the text makes clear, the ultimate touchstone of the Fourth Amendment is reasonableness."[183] The Court, in fact, has spoken about reasonableness as the "touchstone of" the Fourth Amendment in at least twenty-eight cases.[184]

[182] Cynthia Lee, *Reasonableness with Teeth: The Future of the Fourth Amendment Reasonableness Analysis*, 81 MISS. L.J. 1133, 1133–34 (2011).

[183] Riley v. California, 134 S. Ct. 2473, 2482 (2014) (citing Brigham City v. Stuart, 547 U.S. 398, 403 (2006)) (internal quotation marks omitted).

[184] *Riley*, 134 S. Ct. at 2482; ("As the text makes clear, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"); *Stuart*, 547 U.S. at 308 ("the Fourth Amendment's ultimate touchstone is "reasonableness," and "the ultimate touchstone of the Fourth Amendment is 'reasonableness'"); Cnty. of L.A. v. Mendez, 137 S. Ct. 1539, 1546 (2017); Birchfield v. North Dakota, 136 S. Ct. 2160, 2186 (2016) ("reasonableness is always the touchstone of Fourth Amendment analysis"); City of Los Angeles v. Patel, 135 S. Ct. 2443, 2458 (2015) ("the ultimate touchstone of the Fourth Amendment is 'reasonableness'"); Rodriguez v. U.S., 135 S. Ct. 1609, 1617–18 (2015) ("As the text indicates, and as we have repeatedly confirmed, the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"); Heien v. North Carolina, 135 S. Ct. 530, 536 (2014) ("the ultimate touchstone of the Fourth Amendment is 'reasonableness'"); Fernandez v. California, 134 S. Ct. 1126, 1132 (2014) ("the ultimate touchstone of the Fourth Amendment is 'reasonableness'"); Bailey v. U.S., 568 U.S. 186, 211 (2013); Maryland v. King, 569 U.S. 435, 436 (2013) (citing Samson to say that the ultimate touchstone of the Fourth Amendment is "reasonableness, not individualized suspicion."); Missouri v. McNeely, 569 U.S. 141, 167 (2013) ("the ultimate touchstone of the Fourth Amendment is 'reasonableness'"); Kentucky v. King, 563 U.S. 452, 459 (2011) ("[t]he ultimate touchstone of the Fourth Amendment is 'reasonableness'"); Michigan v. Fisher, 558 U.S. 45, 47 (2009) (per curiam) ("the ultimate touchstone of the Fourth Amendment," we have often said, "is 'reasonableness'"); Samson v. California, 547 U.S. 843, 855, n.4 (2006) ("The touchstone of the Fourth Amendment is reasonableness, not individualized suspicion"); Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cty. v. Earls, 536 U.S. 822, 822 (2002); Atwater v. City of Lago Vista, 532 U.S. 318, 360 (2001) (O'Connor, J., dissenting) (quoting Mimms to say that "It is beyond cavil that "[t]he touch stone of our analysis under the Fourth Amendment is always 'the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security.'"); United States v. Knights, 534 U.S. 112, 118 (2001) ("The Fourth Amendment's touchstone is reasonableness" and "The touchstone of the Fourth Amendment is reasonableness"); United States v. Ramirez, 523 U.S. 65, 66 (1998) ("Such

In contrast to strict liability, reasonableness is also at the core of negligence standards. Negligence standards build on the idea of reasonable care.[185] This connection makes it puzzling that the third party doctrine operates like a strict liability standard. The dichotomy contained within the third party doctrine is out of sync with the underlying constitutional doctrine. Fourth Amendment case law should move to a negligence standard. To do that, it could rely on social interactions.

C. A Proposal: Normal Social Interactions Rule

1. *Non-Dichotomous Privacy in Fourth Amendment Law*

Rather than centering around the choice to expose information to third parties, the Fourth Amendment jurisprudence should make use of what constitutes normal social interactions to define privacy's scope.

In other words, the relevant question should be what really reduces the standard deviation of people's beliefs further and what does not. This would both better protect privacy and be more faithful to the aims of the Fourth Amendment. In our model, disclosing information to one party has only a small effect on an individual's overall privacy. If Abby tells Ben a secret, but not Caroline, then Ben's bell curve will become tighter, but Caroline's will not. Abby's overall privacy would be affected very little. But if someone assumed that, just because Abby told that to Ben, she agrees on telling it to anyone else, she would suffer significant privacy harm.

execution is governed by the general touchstone of reasonableness that applies to all Fourth Amendment analysis"); Maryland v. Wilson, 519 U.S. 408, 411 (1997); Ohio v. Robinette, 519 U.S. 33,–34 (1996) ("The Amendment's touchstone is reasonableness, which is measured in objective terms by examining the totality of the circumstances." *Id.* at 34. "We have long held that the 'touchstone of the Fourth Amendment is reasonableness.'") *Id.* at 39; Florida v. Jimeno, 500 U.S. 248, 250 (1991) ("The touchstone of the Fourth Amendment is reasonableness"); Illinois v. Rodriguez, 497 U.S. 177, 185 (1990); Maryland v. Garrison, 480 U.S. 79, 87 (1987); New Jersey v. T.L.O., 469 U.S. 325, 346 (1985); Michigan v. Long, 463 U.S. 1032, 1051 (1983); Pennsylvania v. Mimms, 434 U.S. 106, 108–09 (1977) ("The touchstone of our analysis under the Fourth Amendment is always 'the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security'"); Hill v. California, 401 U.S. 797, 804 (1971); Cty of Los Angeles, Calif. V. Mendez, 137 S. Ct. 1539, 1546 (2017) (citing Birchfield to say that "Reasonableness is always the touchstone of Fourth Amendment analysis"); *see also* California v. Ciraolo, 476 U.S. 207, 211 (1986) ("The touchstone of the Fourth Amendment analysis is whether a person has a constitutionally protected reasonable expectation of privacy, which involves the two inquiries of whether the individual manifested a subjective expectation of privacy in the object of the challenged search, and whether society is willing to recognize that expectation as reasonable"); Oliver v. United States, 466 U.S. 170, 177 (1984) ("Since Katz v. Unites States, supra, the touchstone of Fourth Amendment analysis has been whether a person has a 'constitutionally protected reasonable expectation of privacy.'").

[185] Gregory C. Keating, *Reasonableness and Rationality in Negligence Theory*, 48 STAN. L. REV. 311, 312 (1996).

The dichotomous conception of privacy (which primarily, but not necessarily, results in concealment) should be replaced with a continuous, and therefore more complete, account of privacy. Social norms are already at the core of Fourth Amendment doctrine,[186] but the third party doctrine undermines their importance. The account of privacy presented here shows that it is mistaken to think that because someone is willing to reveal information to an intermediary, she is also willing to risk revealing to the public. Changing this assumption would transform the definition of a reasonable expectation of privacy under the *Katz* rule from the third party doctrine to an analysis of normal social interactions.

This idea of normalcy relates to the conception of privacy we outlined above. When Abby discloses information to Ben, she knows it will shrink Ben's posterior, and she takes this privacy loss into account in her decision to disclose. Suppose she understands that Ben is likely to repeat the information. Then when she made her decision, she would *also* have incorporated that *additional* utility loss into her cost of disclosure. Social norms about information sharing are a way of determining the likelihood that Ben will repeat the information. Therefore, these norms reflect the fact that Abby had *already* taken that additional (likely) privacy loss into account in making her disclosure decision. This means that she is acting optimally.

This idea of normalcy is intrinsically tied to the negligence standard discussed above. If Abby shares personal information with Ben in a way that it would be normal for Ben to disclose it (either widely or to a single individual) then Abby would have been negligent in her actions and would not enjoy Fourth Amendment protection over that information. She would no longer have a reasonable expectation of privacy over it. However, if Abby conveys information to Ben in a way that it would not be normal for Ben to disclose it (for example, because Ben is her therapist), then Abby would have been diligent in her actions and would have a Fourth Amendment protection over the information.

As the logical consequences of the third party doctrine look increasingly untenable, a more nuanced concept of information privacy is starting to permeate the Court's Fourth Amendment privacy case law.[187] This is true despite the fact that the Court is still lacking a concrete framework for this move. In *United States v. Jones*, for example, in deciding the legitimacy of GPS tracking, the Court went beyond asking what had been exposed to the public and found that, absent a warrant,

[186] Colb, *supra* note 139, at 124.

[187] *See* Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 431–32 (2013).

such surveillance—even in public—violates the Fourth Amendment.[188] Because Jones had 'shared' his location with others, applying the third party doctrine in the case would have led to the opposite conclusion that Jones had no reasonable expectation of privacy regarding his location.

Furthermore, the concurrent opinions in *Jones* more directly limit the doctrine by stating that precise and pervasive monitoring of one's location in public violates the Fourth Amendment even without trespass.[189] In her opinion, Sotomayor noted that

> [m]ore fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[190]

In *Riley v. California*, applying the doctrine would have led to the conclusion that the information was not private because Riley was receiving calls from someone else.[191] The Court stated that "the ultimate touchstone of the Fourth Amendment is reasonableness"[192] and focused on whether the search was necessary to prevent the destruction of evidence.[193]

Reconciling Katz with the third party doctrine is a puzzle. One approach is to view the third party doctrine as protecting privacy as it relates to copies of information, not as it relates to facts. Whereas in Miller, for example, the bank had its own copy of the information, tapping Katz's telephone involved generating a new copy of that conversation. Like the bank in Miller, intermediaries have their own copies of information so, under this view of the third party doctrine, the Fourth Amendment does not protect them.[194] This is consistent with the idea that the Fourth Amendment—and by extension the third party doctrine—is concerned with the evidence about information, not with the information itself. Under the model, evidence, including information that is really being sought is the defendant's "type" (normally, whether the defendant is guilty). Because the third party doctrine is about

[188] United States v. Jones, 565 U.S. 400, 404 (2012).

[189] *Jones*, 565 U.S. at 413–21 (Sotomayor, J., concurring) (Alito, J., concurring) (note that the two concurrent opinions amount for five justices. If issued together, they would have constituted a majority opinion against the third party doctrine).

[190] *Id.* at 417 (citation omitted).

[191] *See generally* Riley v. California, 134 S. Ct. 2473 (2014). Note that Katz was also speaking on the phone when the Court found that he had a reasonable expectation of privacy. Katz v. United States, 389 U.S. 347, 348 (1967).

[192] *Riley*, 134 S. Ct. at 2482 (citing Brigham City v. Stuart, 547 U.S. 398 (2006)).

[193] *Riley*, 134 S. Ct. at 2482 (citing Chimel v. California, 395 U.S. 752 (1969)).

[194] Conversation with Kathy Strandburg on Nov. 29, 2017. We thank her for pointing out this interpretation to us.

evidence, it is natural that its primary concern be with protecting signals, rather than about protecting the underlying information. At the same time, however, there is no basis for distinguishing, either in terms of the expected informativeness of signals or in terms of the disutility to target persons, between existing copies and other signals for the purposes of Fourth Amendment protection. When Caroline observes a signal about Abby, it makes no difference to Abby whether that signal is a copy of a signal that Ben had already seen, or whether it was a new signal. Both cases have the exact same effect on Abby's privacy with respect to Caroline.

Both *Jones* and *Riley*, as well as most of the academic proposals regarding the third party doctrine so far, have focused on adapting the doctrine to the new realities of the digital world. What we have shown here is that the underlying problem is deeper than that. Technology can challenge legal doctrine in two distinct ways. It can do so by presenting a new problem that was absent before, like artificial intelligence algorithms. Alternatively, it can make pre-existing problems more salient, like ease of copying copyrighted works. Whereas most criticisms of the third party doctrine place it in the first category, our approach shows that it really belongs in the second. The third party doctrine has always implied a misunderstanding of how society reacts to sharing information. The emergence of intermediary-based communications did not create a new problem, but simply increased the severity and the salience of its already existing problem. The best legal response, then, is not to adjust the doctrine to intermediaries but rather to use the opportunity to replace it with something different that avoids this fundamental problem.

In sum, the understanding of a reasonable expectation of privacy should shift from the status quo—a de facto a strict liability rule—to a negligence rule. The level of care employed in the negligence standard should then look to how social interactions normally function. Understanding normal social interactions will allow us to see what expectations a person could reasonably have after sharing information with another in the way she did.

2. *Normal Social Interactions and Social Expectations*

Defining reasonable expectations of privacy through the idea of normal social interactions relates Fourth Amendment privacy law to the common law of privacy in torts. In *Dietemann v. Time*, for example, the Court found that there was intrusion upon seclusion because of the subterfuge of the means used to collect information.[195] They were not part of normal social interactions, just as Scalia observed in *Kyllo* that gathering information with thermal technology was not.[196] Neither is the use of a pen register, the search method employed in *Smith*.[197] Our proposed rule therefore relates privacy, rather than to a strict liability standard, to the idea of the reasonable person of ordinary prudence.

Law often defines people's expectations. People expect others to walk on the sidewalk in front of their homes, for example, but not on their front yards. However, to determine their privacy expectations, people do not look so much at what the law allows but rather evaluate what actions are normal in the interaction that is taking place. For example, while it is normal to consider what is and what is not at plain view,[198] people typically do not look to the applicable administrative law regulations.[199] What is "in plain view" is determined by social uses, not the law, in the same way that what is "in public" for the common law of privacy is determined by what is accessible to the public, not by the formality of whether the property was private or public.[200]

Returning to the two distinct interests protected by privacy law, privacy and reputation,[201] it is clear that the Fourth Amendment is concerned with the former. The third party doctrine has privacy, not reputation, as a conflicting interest limiting its scope. Inasmuch as the Fourth Amendment cases are the constitutional equivalent of the common law intrusion upon seclusion cases, it is easy to see how the latter would look if the third party doctrine was applied to them. While *Nader*, *Dietemann*, and *Shulman* were all successful in their intrusion claims, under the third party doctrine (replacing "authorities" for "other

[195] Dietemann v. Time, Inc., 449 F.2d 245,247 (9th Cir. 1971).

[196] In *Nader v. General Motors Corporation*, on the other hand, the Court stated:

> information about the plaintiff which was already known to others could hardly be regarded as private to the plaintiff. Presumably, the plaintiff had previously revealed the information to such other persons, and he would necessarily assume the risk that a friend or acquaintance in whom he had confided might breach the confidence.

255 N.E.2d 765, 770 (N.Y. 1970); *see also* Kyllo v. United States, 533 U.S. 27 (2001).

[197] Smith v. Maryland, 442 U.S 735 (1979).

[198] For the plain view doctrine, see generally Harris v. United States, 390 U.S. 170 (1984). For its extension to the open fields doctrine, see generally Oliver v. United States, 466 U.S. 170 (1984). For its limit, the curtilage doctrine, see generally United States v. Dunn, 480 U.S. 294 (1987).

[199] A case in which the law could create an expectation of privacy is when privacy is contractually agreed. Courts have generally stopped short of recognizing this due to the third party doctrine. DANIEL J. SOLOVE, NOTHING TO HIDE—THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 108–09 (2011). However, in some cases, such as *United States v. Warshak*, contracts have been used to define expectations of privacy when they can be used against it, when there is a clear provision in terms of service reserving a right. 631 F.3d 266, 320 (6th Cir. 2010).

[200] For example, one can be "in public" in a shopping mall, or in one's balcony, but "in private" on the side of the road behind some protection that impedes others from seeing one.

[201] *See supra* Subpart III.A.

third parties"), none of the plaintiffs would have been successful. Thinking of intrusion upon seclusion cases such as *Nader*, *Dietemann*, and *Shulman* in terms of the third party doctrine sheds light on its underlying problems.

Carpenter illustrates this point as well. While Carpenter might have been aware that his telephone provider can identify his location, he surely would not have thought it normal for this information to be passed on along to other parties. As such, under a normal social interactions rule, Carpenter would likely be held to have taken due care regarding his geolocation information. In contrast, a ruling in Carpenter that effectively established a strict liability rule would create incentives for people to take inefficient and socially undesirable levels of care regarding their geolocation. The social outcome of having every person take such high levels of care, leaving their phone at home every time they do not want to be followed by anyone, is likely to outweigh the social benefit of not having to ask a judge for a warrant when this information is valuable in criminal procedure.[202]

Much of the discussion of the case has centered around whether the third party doctrine extends to long term tracking.[203] But the case is an opportunity to do something more useful and important: recognizing how longer term tracking is yet another example of the flaw at the root of the third party doctrine. Instead of relying on voluntary disclosure to a single party to form a conclusive presumption that the disclosing party has no reasonable expectation of privacy (thereby taking us out of the general Fourth Amendment approach of "reasonableness"), we should consider the effect of voluntary disclosure as part of the general reasonableness inquiry. That is: Was it reasonable to assume that the third party would disclose the information to other third parties? Is the government's search regime otherwise reasonable?

CONCLUSION

We presented a simple characterization of information privacy that, aims to capture the impact of information on privacy loss and privacy harm. Our model is designed to emphasize the aspects of privacy that are relevant for law, particularly in light of technological innovations that changed the way in which people acquire, store, and disseminate

[202] *Cf.* Balkin, *supra* note 136, at 1231 (explaining, for the proposal of information fiduciaries that "[t]his conclusion does not mean that the government may not obtain the information at all. The government may still use warrants upon a showing of probable cause. Or the information may fall under one of the exceptions to the warrant requirement.")

[203] Transcript, *supra* note 163, at 4 (petitioner's attorney stating that "the rule we seek is that longer-term periods or aggregations of cell site location information is a search and requires a warrant").

information. We then apply our model to the privacy tort and draw an analytical and doctrinal distinction between the two types of interests it protects. We then turn to the third party doctrine, and use insights from our model to overcome what is perhaps the most criticized element of Fourth Amendment law.

In the tort law context, we use the model to distinguish between privacy and reputational interests in privacy law. While only the first is a true privacy interest, the second can be protected by privacy *rules*, even if it is not itself a privacy interest. We then divided the four privacy torts between these two interests, and showed how this model can help to make sense of the existing doctrine. Finally, we analyzed how this impacts the interaction between privacy and the First Amendment, the role of truth as a defense against a privacy claim, and the evidentiary requirements of the privacy tort.

The model also helps identify a root problem for the third party doctrine and clarifies why some of the existing suggestions to overcome its counterintuitive results—such as the existence of options and the concept of information fiduciaries—might be insufficient. We then use insights from the model to propose a better way forward, which is consistent with the concurrent opinions in *Jones* and the majority in *Riley*: to move from a strict liability rule to one based on what is reasonably expected from social interaction. *Carpenter* represents an opportunity for the Court to alter the current doctrine dispensing with the third party doctrine and replacing it with a substantive view of reasonable expectations of privacy of the Fourth Amendment.

The applications of the model discussed in this paper represent just a few examples where differentiating between privacy loss and privacy harms has cognizable legal consequences. As privacy concerns become increasingly important, and problems involving privacy loss become more prevalent, our model can serve as a useful tool in evaluating privacy harms in other areas of the law as well.

Mathematical Appendix

A. The Baseline Model

1. Formalization

Suppose that there is a continuum of individuals, each endowed with a type θ on the interval *I*. Denote A's type as θ^*. Define B's prior about A's type as $\pi(\theta)$, where $\pi(\theta)$ is a probability density function (pdf).[204] For simplicity, assume that $\pi(\theta) > 0 \forall \theta \in I$.[205] Suppose further that B can observe *N* independent and identically distributed unbiased signals about A. Denote each signal *j* in B's information set as X_j, and let the realization of each signal *j* be x_j. Denote $\mathbf{X} = [X_1, X_2, ..., X_N]^{\mathrm{T}}$ and $\mathbf{x} = [x_1, x_2, ..., x_N]^{\mathrm{T}}$. Since the signals are unbiased, we have that $E[x_i] = \theta^* \forall x_i \in \mathbf{x}$.

Define the joint conditional pdf of $\mathbf{X}$ as $h(\mathbf{x} \mid \theta) = f(x_1 \mid \theta) f(x_2 \mid \theta) ... f(x_N \mid \theta)$. Using standard Bayesian updating,[206] B's posterior pdf is given by

$$k(\theta \mid \mathbf{x}) = \frac{h(\mathbf{x} \mid \theta)\pi(\theta)}{g_1(\theta)}$$

where $g_1(\theta) = \int_{-\infty}^{\infty} h(\mathbf{x} \mid \theta)\pi(\theta)\partial\theta$. Denote the standard deviation of this posterior pdf after observing N signals by σ_N.

We model A's privacy as σ_N, the standard deviation of B's posterior given the *N* signals in B's information set. For any $0 \le k \le N$, as B's information set increases from $(N-k)$ signals to *N* signals, A's privacy loss is given by $L(A, N, k) = \sigma_{N-k} - \sigma_N$.

2. *Baseline Model*

In our baseline model, we assume that both B's prior and the signals that he observes are drawn from a normal distribution, which allows us to use standard formulas to characterize B's posterior distribution. Doing so implies some loss of generality,[207] but allows us to generate clearer intuitions. Later, we relax some of these assumptions, and the main intuitions are unchanged.

Suppose that while B cannot observe A's type directly, he knows that the distribution of types in the population as a whole is normal[208] with a

[204] For an introduction to probability density functions, see ROBERT V. HOGG, JOSEPH W. MCKEAN & ALLEN THORNTON CRAIG, INTRODUCTION TO MATHEMATICAL STATISTICS 45 (6th ed. 2005).

[205] This ensures that A's type could lie anywhere on *I* with at least some positive probability.

[206] HOGG ET AL., *supra* note 204, at 579–89 (6th ed. 2005).

[207] The loss of generality come from the fact that we have specified the shapes of the distributions.

[208] A normal distribution is also known as a Gaussian distribution, or a bell curve.

mean of μ_0 and a standard deviation of σ_0.[209] This implies that the interval *I* is $(-\infty, \infty)$.[210]

Before he learns anything about A, the best B can do is assume that she looks like the population as a whole. His *prior* is that her type is drawn from the distribution of types in the population. As a result, his best guess about her type is that it is equal to μ_0, the population mean.

Now suppose that B can also observe informative signals about A. In particular, suppose that B observes N independent and identically distributed signals drawn from a normal distribution centered around θ^* with a standard deviation of *s*. Let

$$\bar{x}_N = \frac{1}{N}\sum_{j=1}^{N} x_j$$

be the sample mean, and s_N the standard deviation of x_N.

As B observes signals, he updates his beliefs and forms a *posterior* belief about A's type. In this example, it can be shown that B's posterior distribution is also a normal distribution, with a mean of

$$\mu_N = \frac{\sigma_0^2}{\sigma_0^2 + {s^2}/{N}}\bar{x}_N + \frac{{s^2}/{N}}{\sigma_0^2 + {s^2}/{N}}\mu_0$$

and a standard deviation

$$\sigma_N = \sqrt{\frac{\left({s^2}/{N}\right)\sigma_0^2}{\left({s^2}/{N}\right) + \sigma_0^2}} = \sqrt{\frac{s^2\sigma_0^2}{s^2 + N\sigma_0^2}}.$$

The mean of the posterior, μ_N, is a weighted average of the prior and the observed signals. As the number of signals increases, *ceteris paribus*, the posterior converges toward the sample mean. More importantly, as the number of signals increases, the standard deviation

[209] This distribution has a probability density function $\pi(\theta) = \frac{1}{\sqrt{2\pi\sigma_0^2}}\exp\left\{-\frac{(\theta-\mu_0)^2}{2\sigma_0^2}\right\}$.

[210] This comes from the fact that the normal distribution has infinite support on the real line. In the case of a prior with finite support, *I* would be some finite interval. Changing this interval has no effect on the intuition of the model.

of the posterior, σ_N, falls.[211] Eventually, as N approaches infinity, the standard devia̲tion falls to zero. Moreover, as N approaches infinity, the sample mean x_N converges to the true mean θ^*. At that point, A has no privacy at all.

3. *Preferences over Privacy*

Formally, A's utility function over privacy is defined as a function that is increasing and concave in the standard deviation of B's posterior distribution. This captures the intuition that individuals prefer more privacy to less (other things equal), but they do so at a decreasing rate. Let σ be the standard deviation of the distribution, and let y be a composite good. The utility function is defined as $U(\sigma, y)$, where $\frac{\partial U(\sigma,y)}{\partial \sigma} > 0$ and $\frac{\partial^2 U(\sigma,y)}{\partial (\sigma)^2} < 0$. The curve in Figure 2 below represents a utility function for privacy that satisfies these criteria.

[211] To see this, notice that $\frac{\partial \sigma_N}{\partial N} < 0$.

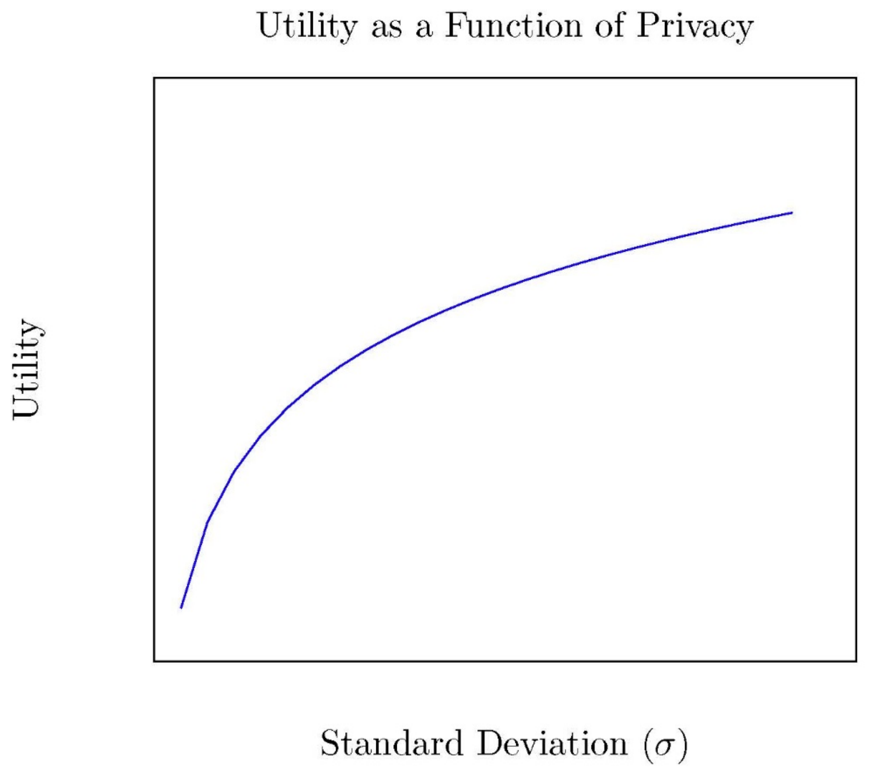

Figure 2: Example of a privacy utility function

4. *Preferences over Privacy vs. Preferences over Signals*

We noted in Part II.B.1 that, while Abby's utility over *privacy* is assumed to be concave, her utility over *information* may not be.

To see this formally, notice that we can write

$$\frac{\partial U(\sigma_N, y)}{\partial N} = \frac{\partial U(\sigma_N, y)}{\partial \sigma_N} \frac{\partial \sigma_N}{\partial N}$$

and

$$\frac{\partial^2 U(\sigma_N, y)}{\partial N^2} = \frac{\partial^2 U}{\partial {\sigma_N}^2} \left(\frac{\partial \sigma_N}{\partial N} \right)^2 + \frac{\partial U}{\partial \sigma_N} \frac{\partial^2 \sigma_N}{\partial N^2}.$$

These two equations characterize how a change in the number of signals that Ben observes affects Abby's utility. The former, which represents the derivative with respect to *N*, characterizes the effect of an increase in the number of signals on her utility, while the latter, which represents the second derivative, characterizes the effect of such a change on the *slope* of that function. It can be shown that under our simplifying assumptions from Subpart A.2, Abby's utility is decreasing in the number of signals Ben receives.[212] More importantly, under the same conditions, the effect of *N* on the second derivative is, in general, indeterminate. This implies that, while Abby has concave preferences over *privacy*, she may have convex preferences over *signals*.

B. EXTENSIONS OF THE MODEL

We now discuss a few extensions of the basic model. In the above discussion, we assumed that B knew the population distribution of θ, and that A had full information. We now relax these assumptions.[213]

1. *Uninformed Prior*

What if B does not know the population distribution? For example, perhaps he honestly knows nothing at all about how types are distributed in the population. Alternatively, perhaps it has never occurred to him to even think about this until now.

[212] To see this, recall that $\sigma_N = \sqrt{\frac{s^2\sigma_0^2}{s^2 + N\sigma_0^2}}$ so that $\frac{\partial \sigma_N}{\partial N} < 0$.

[213] We also assumed that both the signals and the prior were normal and independent and identically distributed. Both of these assumptions can be relaxed.

The assumption that the population distribution and the signal generating process are normal is made for simplicity. Conceptually, nothing relies on this assumption. Relaxing this assumption, we lose the closed-form solution for the both the mean and standard deviation of the posterior. The latter is more inconvenient as it, in turn, means that we lose the closed from solution for A's privacy loss. While this loss is inconvenient, it is not fatal. For any given prior $\pi(\theta)$, and any given conditional joint probability density function of X $h(\boldsymbol{x}|\theta)$, we can simply calculate the posterior $k(\theta|\boldsymbol{x})$. Define σ_0 as the standard deviation of $\pi(\theta)$, and σ_N as the standard deviation of the posterior. Then A's privacy loss in moving from the prior to the posterior is given by $L(A, N, k) = \sigma_0 - \sigma_N$. For any given $\pi(\theta)$ and $h(\boldsymbol{x}|\theta)$ these standard deviations can be computed using a standard statistical formula. *See, e.g.*, ROBERT V. HOGG ET AL., INTRODUCTION TO MATHEMATICAL STATISTICS 59-60 (6th ed. 2005).

The assumption of independent and identically distributed signals is another mathematical convenience. If instead the signals are independent and not identically distributed, we will simply have a different function for $h(\boldsymbol{x}|\theta)$. Conceptually, nothing will change. Even the independence assumption is also not particularly important. We can accommodate arbitrary correlations between the signals by simply redefining the $h(\boldsymbol{x}|\theta)$ function to

$$h(\boldsymbol{x}|\theta) = f(x_1|\theta)f(x_2|\theta, x_1)\ldots f(x_N|\theta, x_1, x_2, \ldots, x_{n-1})$$

Here again, while this accommodation may introduce tedious calculations, the interpretations and the intuitions are unchanged.

In such cases, we propose that the most appropriate prior is a uniform distribution. This puts equal weight on every possible outcome, which seems the most reasonable way to think of the problem in the absence of any other information.

2. *Uncertainty*

What if A is uncertain about B's prior and/or posterior? In other words, what if A does not know with certainty how much B already knows about her? Alternatively, (or additionally), what if A does not know with certainty how much B will learn about her from observing k additional signals?

We can address both of these issues by borrowing from the machinery already developed for dealing with risk and uncertainty in economics. In particular, we assume that $U(\sigma, y)$ is a well-defined Von Neumann-Morgenstern utility function. Because A is uncertain about σ_N and σ_{N-k}, she simply uses her best guess about how likely any particular value of σ_N and σ_{N-k} are. Her utility is then given by her expected utility over these possible values.[214]

3. *Multidimensional Types and Privacy as Context*

In the baseline model, we assumed a unidimensional type θ on the (unidimensional) interval *I*. The model can easily be generalized to allow multidimensional types. For example, suppose that θ_A P-dimensional vector representing *A*'s type, where each of the P elements represent a sub-type. The signals that B observes are now P-dimensional vectors, and rather than having a single standard deviation, we have a P-by-P covariance matrix Σ. A's privacy loss is now defined with respect to each sub-type. For each p in P, A's privacy loss is now the incremental reduction in the square root of the p$^{\text{th}}$ diagonal entry of Σ.

Similarly, the baseline model focused on the case where there is only one homogenous class of observer, and modeled both privacy loss and utility over privacy in a single context. While we believe that this simplification is a useful benchmark, it is straightforward to generalize our model to one that incorporates privacy in different contexts. Rather than defining the utility function over a single standard deviation term,

[214] For example, suppose A believes that there is a 50% chance that σ_{N-k} is 0.5, and a 50% chance that it is .75. Suppose that in either case, there is a 25% chance that after receiving k additional signals, the variance of B's posterior will fall by 50%, and a 75% chance that it will fall by 25%. A's expected utility ex ante is therefore $\frac{1}{2}U(0.5, y) + \frac{1}{2}U(0.75, y)$' and her expected utility ex post is $\frac{1}{2}\left[\frac{1}{4}U(.5*.5, y) + \frac{3}{4}U(.5*.75, y)\right] + \frac{1}{2}\left[\frac{1}{4}U(.75*.5, y) + \frac{3}{4}U(.75*.75, y)\right]$, or $\frac{1}{8}U(.25, y) + \frac{1}{2}U(.375y) + \frac{3}{8}U(.5625y)$.

we can generalize it to be defined over several terms. Formally, if an individual is concerned with privacy in P different contexts, the utility function is simply $U(\sigma\ , y)$, where

$$\frac{\partial U(\sigma_p, y)}{\partial \sigma_p} > 0$$

and

$$\frac{\partial^2 U(\sigma_p, y)}{\partial (\sigma_p)^2} < 0$$

some $p\ \in P$, $\sigma = \left[\sigma_1, \sigma_2, ..., \sigma_P\right]^{\mathrm{T}}$ is a P-dimensional vector, and σ_p represents the standard deviation in each context $p\ \in P$. Figure 3 illustrates a simple example of a utility function that satisfies these characteristics where *P=2*.

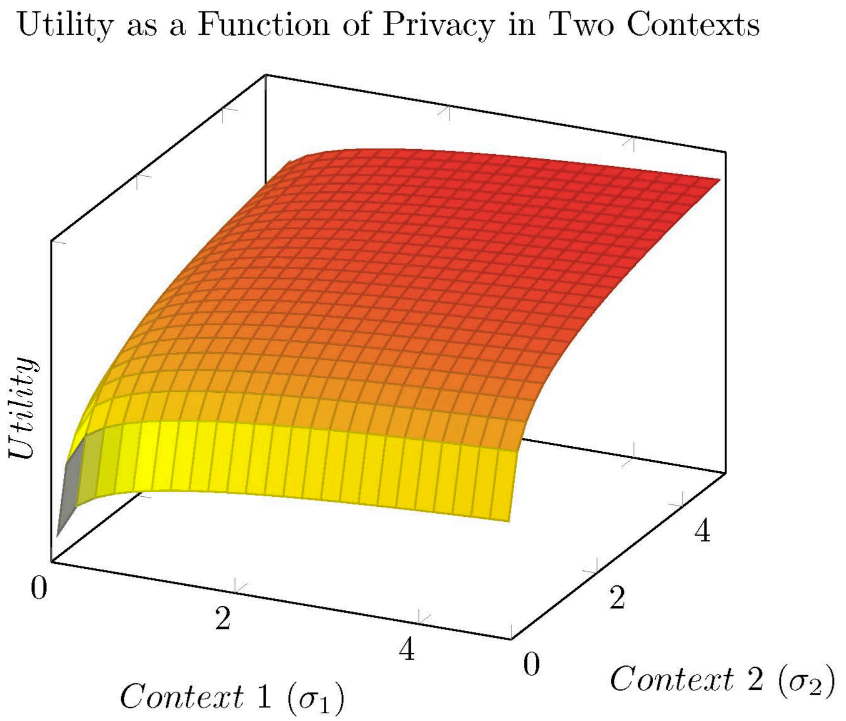

Figure 3: Example Utility Function Incorporating Context

This generalization allows for a tremendous amount of flexibility. Not only does it allow the individual to put different weights on privacy in different contexts, it also allows for preferences that depend on the interactions between privacy in different contexts. For example, an individual might care about relative levels of privacy, or might only care about privacy in certain contexts, but not others.

This generalization to contextual privacy is mathematically equivalent to our formalization of multidimensional types. We view this as a feature of the model. While there is no question that the conceptual meaning behind the two formalizations are distinct, the mathematical machinery we develop allows us to capture both. This makes our model both adaptable and parsimonious.