Taxonomy of Privacy Issues

Since it may be helpful to the Privacy Policy Subcommittee's upcoming discussions, this document summarizes Professor Daniel Solove's *A Taxonomy of Privacy*.[1] The article attempts to identify precisely each type of privacy problem and describe how the problems are related to each other. In addition to the dignitary harms caused by breaches of privacy, Professor Solove discusses two of what he labels "architectural" problems. First, he explains that poor data management can make people more vulnerable to harm (i.e., injures to the individual's dignity, person, or financial well-being). Second, he points out that a particular activity can upset the balance of social or institutional power in undesirable ways. The classic example of the latter problem is the chilling effect of various information-gathering activities. Professor Solove's four basic groups of activities are outlined below; his entire article, originally published in the University of Pennsylvania Law Review is attached.

Information Collection

Surveillance

Surveillance is the watching, listening to, or recording of an individual's activities.

Potential harm

Surveillance is a tool of social control. The mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition. Too much social control can adversely impact freedom, creativity, and self-development.

Interrogation

Interrogation includes various forms of questioning or probing for information. It resembles *intrusion* in its invasiveness and often involves the divulging of concealed information like *disclosure*. It is also related to *surveillance* in that it may involve the involuntary gathering of information.

Potential harm

Harms associated with interrogation arise from the degree of coerciveness involved. People often feel some degree of compulsion because not answering might create the impression that they have something to hide. Interrogation forces people to be concerned about how they will explain themselves or how their refusal to answer will appear to others. Historically, interrogation has been employed to impinge upon freedom of association and belief.

Information Processing

Identification

Identification is the act of connecting data to particular individuals. Identification enables *surveillance* by facilitating the monitoring of a person.

Potential harm

Identification increases the government's power to control individuals. It can inhibit one's ability to be anonymous. Anonymity is important in so far as it protects people from bias based on their identities and enables people to vote, speak, and associate more freely by protecting them from the danger of reprisal. Today, identifying yourself is the same as linking yourself to your digital portrait.

Secondary use

Secondary use is the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent.

Potential harm

Secondary use creates dignitary harm, in that it thwarts people's reasonable expectations about how the data they give out will be used. The potential for secondary use generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability. Secondary use of information also creates architectural problems. Specifically, data may be misunderstood when it is removed from its original context.

[1] Solove, Daniel J., "A Taxonomy of Privacy" 154 U. PA. L. REV. 477, 490 (Jan. 2006).

Information Processing (continued)

Insecurity

Insecurity involves carelessness in protecting stored information from leaks and improper access. Glitches, security lapses, abuses, and illicit uses of personal information all fall into this category.[2]

Potential harm

Insecurity exposes people to potential future harm, most notably, identity theft. The careless use of data by businesses and the government makes the crime of identity theft much easier.

Exclusion

Exclusion is the failure to provide individuals with notice and input about their records.

Potential harm

Exclusion reduces accountability on the part of government agencies and businesses that maintain records about individuals. This lack of accountability often goes hand-in-hand with *insecurity* in record systems. Additionally, the inability to participate in the maintenance and use of one's information can lead to feelings of powerlessness and frustration. This can be troublesome where important decisions are based upon this personal information.

Aggregation

Aggregation is the gathering together of various pieces of information about a person. Although less direct than *surveillance*, aggregation is another way to acquire information about an individual.

Potential harm

A piece of information here or there is not very telling; but when combined together, these bits and pieces of data begin to form a portrait of a person. Aggregation can cause dignitary harms because of its ability to unsettle an individual's expectations regarding how much information about themselves is revealed to others. Aggregation also creates architectural problems by increasing the power that others have over the individual data subject. Architectural problems emerge where the data compilation used to judge the individual is incomplete or results in a distorted portrait of the person because the information is disconnected from the original context in which it was gathered.

Information Dissemination

Breach of confidentiality

Breach of confidence involves breaking a promise to keep a person's information confidential.

Potential harm

The harm caused by a breach of confidentiality is not simply that information has been disclosed, but that the victim has been betrayed. Protections against breach of confidentiality help promote certain relationships that depend upon trust, such as the relationship between citizens and their government.

Disclosure

Disclosure occurs when certain true information about a person is revealed that impacts the way others judge her character.

Potential harm

The potential harm of disclosure involves the damage to reputation caused by the dissemination. This is different from the harms caused by breaching confidentiality (e.g., the violation of trust in the relationship). Disclosure can be a form of social control that prevents people from engaging in activities that further their own self-development, inhibit people from associating with others, and destroy anonymity, which is sometimes critical for the promotion of free expression. Disclosure can also threaten people's security by making them vulnerable to physical, emotional, financial, and reputational harms. Disclosure can also be harmful where it makes a person a prisoner of her recorded past. People grow and change, and disclosures of information from their past can inhibit their ability to reform their behavior, have a second chance, or alter their life's direction.

---

[2] Professor Solove groups several data quality issues under the *Insecurity* heading. Specifically, he opines that improperly compiled data is a security concern. This is odd since the difficulties of linking data to the correct individual is ordinarily characterized as a data quality issue.

Information Dissemination[3]

Distortion

Distortion consists of the dissemination of false or misleading information about individuals.

Potential harm

Distortion, like disclosure, involves the spreading of information that affects the way society views a person. Both distortion and *disclosure* can result in embarrassment, humiliation, stigma, and reputational harm. They both involve the ability to control information about oneself and to have some limited dominion over the way one is viewed by society. Distortion differs from disclosure, however, because with distortion, the information revealed is false and misleading.[4]

Increased accessibility

Increased accessibility makes information that is already available to the public easier to access.

Potential harm

Unlike disclosure, the harm is not a direct revealing of information to another; nor is confidentiality breached. Rather, increased accessibility enhances the risk of the harms of *disclosure*. Additionally, the potential harms associated with *secondary use* are implicated because easily accessible information can readily be exploited for purposes other than those for which it was originally made publicly accessible.

Invasions

Intrusion

Intrusion concerns invasive acts that disturb one's tranquility or solitude. Intrusion can be caused by physical invasions as well as *surveillance* and *interrogation*.

Potential harm

Solitude is built into society's structure to enhance the quality of life in the public sphere. Specifically, it enables individuals to develop social relationships and pursue artistic, political, and religious ideas that can contribute value to society. The harm caused by intrusion is the interruption of one's activities through the unwanted presence or activities of another person.

Decisional interference

Decisional Interference is governmental intrusion into people's decisions regarding certain matters of their personal lives.

Potential harm

Decisional interference involves unwanted incursion by the government into an individual's decisions about her personal life. This can have a chilling effect on a person's decisions regarding her body, home, and family.

---

[3] Blackmail, exposure, and appropriation have been omitted from this summary because they are unlikely to be implicated in the Privacy Policy Subcommittee's discussions.

[4] Professor Solove states that the inaccurate portrayal of an individual due to true but incomplete data that has been taken out of context is a problem associated with appropriation and secondary use while the use of inaccurately compiled data is more accurately described as distortion. It is unclear whether this bifurcation of harms is a useful tool for privacy policy development purposes.

University of Pennsylvania Law Review

FOUNDED 1852

Formerly
American Law Register

VOL. 154 | JANUARY 2006 | NO. 3

ARTICLES

A TAXONOMY OF PRIVACY

DANIEL J. SOLOVE[†]

Privacy is a concept in disarray. Nobody can articulate what it means. As one commentator has observed, privacy suffers from "an embarrassment of

[†] Associate Professor, George Washington University Law School; J.D. Yale.

A project such as this—one that attempts a taxonomy of the sprawling and complex concept of privacy—cannot be created by one individual alone. I owe an enormous debt of gratitude to many people who provided helpful comments on the manuscript or parts thereof at various stages in its development: Anita Allen, Howard Erichson, Jim Freeman, Robert Gellman, Rachel Godsil, Stan Karas, Orin Kerr, Raymond Ku, Chip Lupu, Jon Michaels, Larry Mitchell, Robert Post, Neil Richards, Michael Risinger, Peter Sand, Heidi Schooner, Paul Schwartz, Lior Strahilevitz, Charles Sullivan, Michael Sullivan, Peter Swire, Robert Tuttle, Sarah Waldeck, Richard Weisberg, and James Whitman. Thanks to Michael Weisberg and Brian Leiter for directing me to useful resources on systematics. I would also like to thank my research assistants, Poornima Ravishankar, Jessica Kahn, and Tiffany Stedman for their excellent assistance. Additionally, I benefited from helpful comments when I presented this paper at a workshop at Washington University and at a conference sponsored by the International Association of Privacy Professionals. The George Washington University School of Law scholarship fund provided generous support for this Article.

meanings." Privacy is far too vague a concept to guide adjudication and lawmaking, as abstract incantations of the importance of "privacy" do not fare well when pitted against more concretely stated countervailing interests.

In 1960, the famous torts scholar William Prosser attempted to make sense of the landscape of privacy law by identifying four different interests. But Prosser focused only on tort law, and the law of information privacy is significantly more vast and complex, extending to Fourth Amendment law, the constitutional right to information privacy, evidentiary privileges, dozens of federal privacy statutes, and hundreds of state statutes. Moreover, Prosser wrote over 40 years ago, and new technologies have given rise to a panoply of new privacy harms.

A new taxonomy to understand privacy violations is thus sorely needed. This Article develops a taxonomy to identify privacy problems in a comprehensive and concrete manner. It endeavors to guide the law toward a more coherent understanding of privacy and to serve as a framework for the future development of the field of privacy law.

INTRODUCTION

In Jorge Luis Borges's illuminating parable, *Everything and Nothing*, a gifted playwright creates breathtaking works of literature, populated with an unforgettable legion of characters, one after the other imbued with a unique, unforgettable personality.[1] Despite his spectacular feats of imagination, the playwright lives a life of despair. He can dream up a multitude of characters—become them, think like them, understand the depths of their souls—yet he himself has no core, no way to understand himself, no way to define who he is. At the end of the parable, before he dies, the playwright communicates his despair to God:

> "I who have been so many men in vain want to be one and myself." The voice of the Lord answered from a whirlwind: "Neither am I anyone; I have dreamt the world as you dreamt your work, my Shakespeare, and among the forms in my dream are you, who like myself are many and no one."[2]

Privacy seems to be about everything, and therefore it appears to be nothing. As one commentator observed:

> It is apparent that the word "privacy" has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts. . . . Like the emotive word "freedom," "privacy" means so many different things to so many different people that it has lost any precise legal connotation that it might once have had.[3]

Lillian BeVier writes: "Privacy is a chameleon-like word, used denotatively to designate a wide range of wildly disparate interests—from confidentiality of personal information to reproductive autonomy—and connotatively to generate goodwill on behalf of whatever interest is being asserted in its name."[4] Other commentators have lamented that privacy is "vague and evanescent,"[5] "protean,"[6] and suf-

---

[1] JORGE LUIS BORGES, *Everything and Nothing*, *in* LABYRINTHS 248 (Donald A. Yates & James E. Irby eds., J.E.I. trans., 1964).

[2] *Id.* at 249.

[3] 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 5.59 (2d ed. 2005).

[4] Lillian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455, 458 (1995) (footnote omitted).

[5] ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 25 (1971) (citation omitted).

fering from "an embarrassment of meanings."[7] "Perhaps the most striking thing about the right to privacy," philosopher Judith Jarvis Thomson has observed, "is that nobody seems to have any very clear idea what it is."[8]

Often, privacy problems are merely stated in knee-jerk form: "That violates my privacy!" When we contemplate an invasion of privacy—such as having our personal information gathered by companies in databases—we instinctively recoil. Many discussions of privacy appeal to people's fears and anxieties.[9] What commentators often fail to do, however, is translate those instincts into a reasoned, well-articulated account of why privacy problems are harmful. When people claim that privacy should be protected, it is unclear precisely what they mean. This lack of clarity creates a difficulty when making policy or resolving a case because lawmakers and judges cannot easily articulate the privacy harm. The interests on the other side—free speech, efficient consumer transactions, and security—are often much more readily articulated. Courts and policymakers frequently struggle in recognizing privacy interests, and when this occurs, cases are dismissed or laws are not passed. The result is that privacy is not balanced against countervailing interests.

Abstract incantations of "privacy" are not nuanced enough to capture the problems involved. The *9/11 Commission Report*, for example, recommends that, as government agencies engage in greater information sharing with each other and with businesses, they should "safeguard the privacy of individuals about whom information is shared."[10] But what does safeguarding "privacy" mean? Without an understanding of what the privacy problems are, how can privacy be addressed in a meaningful way?

Many commentators have spoken of privacy as a unitary concept with a uniform value, which is unvarying across different situations. In contrast, I have argued that privacy violations involve a variety of types

---

[6] Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 234 (1977).

[7] KIM LANE SCHEPPELE, LEGAL SECRETS 184-85 (1988).

[8] Judith Jarvis Thomson, *The Right to Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272, 272 (Ferdinand David Schoeman ed., 1984).

[9] *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1154 (2004) ("[T]he typical privacy article rests its case precisely on an appeal to its reader's intuitions and anxieties about the evils of privacy violations.").

[10] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 394 (2004).

of harmful or problematic activities.[11] Consider the following examples of activities typically referred to as privacy violations:

- A newspaper reports the name of a rape victim.[12]
- Reporters deceitfully gain entry to a person's home and secretly photograph and record the person.[13]
- New X-ray devices can see through people's clothing, amounting to what some call a "virtual strip-search."[14]
- The government uses a thermal sensor device to detect heat patterns in a person's home.[15]
- A company markets a list of five million elderly incontinent women.[16]
- Despite promising not to sell its members' personal information to others, a company does so anyway.[17]

These violations are clearly not the same. Despite the wide-ranging body of law addressing privacy issues today, commentators often lament the law's inability to adequately protect privacy.[18] Courts and policymakers frequently have a singular view of privacy in mind when they assess whether or not an activity violates privacy. As a result, they either conflate distinct privacy problems despite significant

---

[11] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1130 (2002) [hereinafter Solove, *Conceptualizing Privacy*]. In contrast to attempts to conceptualize privacy by isolating one or more common "essential" or "core" characteristics, I concluded that there is no singular essence found in all "privacy" violations. *See id.* at 1095-99 (concluding that "the quest for a common denominator or essence . . . can sometimes lead to confusion").

[12] *See* Florida Star v. B.J.F., 491 U.S. 524, 527 (1989).

[13] *See* Dietemann v. Time, Inc., 449 F.2d 245, 246 (9th Cir. 1971).

[14] *See Beyond X-ray Vision: Can Big Brother See Right Through Your Clothes?*, DISCOVER, July 2002, at 24; Guy Gugliotta, *Tech Companies See Market for Detection: Security Techniques Offer New Precision*, WASH. POST, Sept. 28, 2001, at A8.

[15] *See* Kyllo v. United States, 533 U.S. 27, 29 (2001).

[16] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,461, 82,467 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160 & 164).

[17] *See In re* GeoCities, 127 F.T.C. 94, 97-98 (1999).

[18] *See, e.g.*, Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 208 (1992) ("The American legal system does not contain a comprehensive set of privacy rights or principles that collectively address the acquisition, storage, transmission, use and disclosure of personal information within the business community."); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1611 (1999) ("At present, however, no successful standards, legal or otherwise, exist for limiting the collection and utilization of personal data in cyberspace.").

differences or fail to recognize a problem entirely. Privacy problems are frequently misconstrued or inconsistently recognized in the law. The concept of "privacy" is far too vague to guide adjudication and lawmaking. How can privacy be addressed in a manner that is non-reductive and contextual, yet simultaneously useful in deciding cases and making sense of the multitude of privacy problems we face?

In this Article, I provide a framework for how the legal system can come to a better understanding of privacy. I aim to develop a taxonomy that focuses more specifically on the different kinds of activities that impinge upon privacy. I endeavor to shift focus away from the vague term "privacy" and toward the specific activities that pose privacy problems. Although various attempts at explicating the meaning of "privacy" have been made, few have attempted to identify privacy problems in a comprehensive and concrete manner.[19] The most famous attempt was undertaken in 1960 by the legendary torts scholar William Prosser. He discerned four types of harmful activities redressed under the rubric of privacy:

> 1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
>
> 2. Public disclosure of embarrassing private facts about the plaintiff.
>
> 3. Publicity which places the plaintiff in a false light in the public eye.

---

[19] In 1967, Alan Westin identified four "basic states of individual privacy": (1) solitude; (2) intimacy; (3) anonymity; and (4) reserve ("the creation of a psychological barrier against unwanted intrusion"). ALAN F. WESTIN, PRIVACY AND FREEDOM 31-32 (1967). These categories focus mostly on spatial distance and separateness; they fail to capture the many different dimensions of informational privacy. In 1992, Ken Gormley surveyed the law of privacy. *See generally* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335. His categories—tort privacy, Fourth Amendment privacy, First Amendment privacy, fundamental-decision privacy, and state constitutional privacy—are based on different areas of law rather than on a more systemic conceptual account of privacy. *Id.* at 1340. In 1998, Jerry Kang defined privacy as a union of three overlapping clusters of ideas: (1) physical space ("the extent to which an individual's territorial solitude is shielded from invasion by unwanted objects or signals"); (2) choice ("an individual's ability to make certain significant decisions without interference"); and (3) flow of personal information ("an individual's control over the processing—i.e., the acquisition, disclosure, and use—of personal information"). Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202-03 (1998). Kang's understanding of privacy is quite rich, but the breadth of the categories limits their usefulness in law. The same is true of the three categories identified by philosopher Judith DeCew: (1) "informational privacy"; (2) "accessibility privacy"; and (3) "expressive privacy." JUDITH W. DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 75-77 (1997).

> 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[20]

Prosser's great contribution was to synthesize the cases that emerged from Samuel Warren and Louis Brandeis's famous law review article, *The Right to Privacy*.[21]

However, Prosser focused only on tort law. American privacy law is significantly more vast and complex, extending beyond torts to the constitutional "right to privacy," Fourth Amendment law, evidentiary privileges, dozens of federal privacy statutes, and hundreds of state privacy statutes.[22] The Freedom of Information Act contains two exemptions to protect against an "unwarranted invasion of personal privacy."[23] Numerous state public records laws also contain privacy exemptions.[24] Many state constitutions contain provisions explicitly providing for a right to privacy.[25]

Moreover, Prosser wrote over forty years ago, before the breathtaking rise of the Information Age. New technologies have given rise to a panoply of different privacy problems, and many of them do not readily fit into Prosser's four categories. Therefore, a new taxonomy to address privacy violations for contemporary times is sorely needed.

The taxonomy I develop is an attempt to identify and understand the different kinds of socially recognized privacy violations, one that hopefully will enable courts and policymakers to better balance pri-

---

[20] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

[21] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195-96 (1890).

[22] *See* Anita L. Allen, *Privacy in American Law*, *in* PRIVACIES: PHILOSOPHICAL EVALUATIONS 19, 26 (Beate Rössler ed., 2004) ("American privacy law is impressive in its quantity and scope."). For a survey of the vast scope of the law of information privacy, see DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW (2003).

[23] 5 U.S.C. § 552(b)(6) (2000) (exempting "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy"); *id.* § 552b(c)(7) (exempting disclosure of "investigatory records compiled for law enforcement purposes that "constitute an unwarranted invasion of personal privacy" at open meetings).

[24] *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1160-64 (2002) (examining federal and state freedom of information acts and their exemptions).

[25] *See, e.g.*, ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed."); CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."); FLA. CONST. art. I, § 23 ("Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein.").

vacy against countervailing interests. The purpose of this taxonomy is to aid in the development of the law that addresses privacy. Although the primary focus will be on the law, this taxonomy is not simply an attempt to catalog existing laws, as was Prosser's purpose. Rather, it is an attempt to understand various privacy harms and problems that have achieved a significant degree of social recognition. I will frequently use the law as a source for determining what privacy violations society recognizes. However, my aim is not simply to take stock of where the law currently stands today, but to provide a useful framework for its future development.

THE TAXONOMY

Privacy cannot be understood independently from society. As sociologist Barrington Moore aptly observes, "the need for privacy is a socially created need. Without society there would be no need for privacy."[26] Society is fraught with conflict and friction. Individuals, institutions, and governments can all engage in activities that have problematic effects on the lives of others.

Privacy is the relief from a range of kinds of social friction. It enables people to engage in worthwhile activities in ways that they would otherwise find difficult or impossible. Of course, privacy is not freedom from all forms of social friction; rather, it is protection from a cluster of related activities that impinge upon people in related ways. This taxonomy attempts to identify and organize these problematic activities.[27] These activities often are not inherently problematic or harmful. If a person consents to most of these activities, there is no

---

[26] BARRINGTON MOORE, JR., PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY 73 (1984).

[27] This taxonomy focuses on activities of others that can and do create privacy harms or problems. The full equation for a privacy violation or problem is the existence of a certain activity that causes harms or problems affecting a private matter or activity. This taxonomy focuses on the first part of the equation (harmful or problematic activities) rather than on what constitutes a private matter or activity. Since the question of which matters and activities are private is too culturally variable and contextual, this taxonomy focuses on potentially harmful or problematic activities, about which I believe meaningful generalizations can be made. Despite the fact that the taxonomy limits its focus to the activities that harm or cause problems for private matters or activities, I believe that the taxonomy serves as a useful way for the law to approach and comprehend privacy problems. While the entire "privacy equation" must be worked out in each particular case, the taxonomy aims to carve up the landscape in a way that the law can begin to comprehend and engage. All taxonomies are generalizations based upon a particular focus, and they are valuable only insofar as they are useful. It is my hope that this taxonomy succeeds by this metric.

privacy violation.[28] Thus, if a couple invites another to watch them have sex, this observation would not constitute a privacy violation. Without consent, however, it most often would.

Of course, declaring that an activity is harmful or problematic does not automatically imply that there should be legal redress, since there may be valid reasons why the law should not get involved or why countervailing interests should prevail. As Anita Allen argues, there are certainly times when people should be held accountable for their private activities.[29] The purpose of this taxonomy is not to argue that the law should or should not protect against certain activities that affect privacy. Rather, the goal is simply to define the activities and explain why and how they can cause trouble. The question of when and how the law should regulate can only be answered in each specific context in which the question arises. But attempts to answer this question are increasingly suffering because of confusion about defining the troublesome activities that fall under the rubric of privacy. This taxonomy will aid us in analyzing various privacy problems so the law can better address them and balance them with opposing interests.

In devising a taxonomy, there are many different ways to go about carving up the landscape. I focus on the activities that invade privacy. The purpose of the taxonomy is to assist the legal system in grappling with the concept of privacy. Since the goal of the law is to have privacy protections that best prevent and redress particular problems, we need to first understand the problems in order to evaluate the effectiveness of the protections.

Therefore, my focus is on activities that create problems. I aim to show that these activities differ significantly yet share many commonalities. Privacy is too complicated a concept to be boiled down to a single essence. Attempts to find such an essence often end up being

---

[28] Of course, there remains the issue of what constitutes valid consent, as there are many occasions in which people affirmatively give out information that should not be assumed to be consensual. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1397-98 (2000) (arguing that "people are demonstrably bad at" assessing the risk of future harms that may flow from the piecemeal, otherwise consensual collection of their private data); Schwartz, *supra* note 18, at 1661-64 (1999) (discussing the legal fiction of consent in the context of the Internet, specifically the use of boilerplate consent forms that do not require user agreement before taking effect).

[29] *See* ANITA L. ALLEN, WHY PRIVACY ISN'T EVERYTHING 2, 146 (2003) (discussing tort theories available as recourse for the invasion of privacy in the context of sexual harassment claims).

too broad and vague, with little usefulness in addressing concrete issues. Elsewhere, I have argued that privacy is best understood as a family resemblance concept.[30] As philosopher Ludwig Wittgenstein explained, certain things may not share one common characteristic, but they nevertheless are "*related* to one another in many different ways."[31] Wittgenstein analogized to members of a family, who generally share some traits with each other (eye color, height, facial structure, hair color, etc.), although they may not have one common trait.[32] There is, however, "a complicated network of similarities overlapping and criss-crossing."[33]

The term "privacy" is an umbrella term, referring to a wide and disparate group of related things. The use of such a broad term is helpful in some contexts yet quite unhelpful in others. Consider, for example, the term "animal." "Animal" refers to a large group of organisms—there are mammals, birds, reptiles, fish, and so on. Within each of these groups are subgroups. For some purposes, using the term "animal" will suffice. Suppose Sue asks Bob, "How many animals are in the zoo?" Bob does not need to know anything more specific in order to answer this question. The use of the term "animal" in this sentence will be perfectly clear in most contexts. Now suppose Sue wants Bob to bring her a dog. She will not get very far by saying, "Bring me an animal." Rather, she will specify the kind of animal she wants. Even saying "dog" probably will not be adequate, since Sue probably wants a specific kind of dog. As with the term "animal," there are many times when using the general term "privacy" will work well. But there are times where more specificity is required. Using the general term "privacy" can result in the conflation of different kinds of problems and can lead to understandings of the meaning of "privacy" that distract courts and policymakers from addressing the issues before them.

The taxonomy demonstrates that there are connections between different harms and problems. It is no accident that various problems are referred to as privacy violations; they bear substantial similarities to each other. But we also must recognize where they diverge. The goal is to define more precisely what the problem is in each context—

---

[30] Solove, *Conceptualizing Privacy*, *supra* note 11, at 1096-99.

[31] LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS § 65 (G.E.M. Anscombe trans., 1968) (1958).

[32] *Id.* § 67.

[33] *Id.* § 66.

how it is unique, how it differs from other problems, and how it is related to other types of privacy problems.

Often these problems involve harms to individuals. Certain kinds of harm, such as physical injuries, are very easy to articulate and understand. A privacy violation presents a more difficult case. Warren and Brandeis spoke of privacy as an incorporeal rather than a physical injury. They noted that the law was beginning to recognize nonphysical harms and that "modern enterprise and invention have, through invasions upon [a person's] privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."[34] Privacy, contended the authors, involves "injury to the feelings."[35]

The harms Warren and Brandeis spoke of are dignitary harms. The classic example of such a harm is reputational injury. As Warren and Brandeis noted, defamation law has long recognized and redressed this kind of injury that lowered people in the esteem of others.[36] But as Warren and Brandeis understood, and as this taxonomy will demonstrate, there are other kinds of dignitary harm beyond reputational injury. These are the harms of incivility, lack of respect, or causing emotional angst. At the time Warren and Brandeis wrote, they were concerned that such dignitary harms might strike some as too ethereal to be legally cognizable.[37] Their project aimed to demonstrate that these were genuine harms that were legally cognizable.[38] And they succeeded, as Prosser emphatically demonstrated in 1960 by collecting hundreds of cases.[39]

There is another, more modern kind of privacy problem that does not readily fit with this dignitary understanding of harm. These problems are more structural in nature. I refer to them as "architectural" problems.[40] They involve less the overt insult or reputational harm to

---

[34] Warren & Brandeis, *supra* note 21, at 196.

[35] *Id.* at 197.

[36] *Id.*

[37] *See id.* at 198 (noting that traditionally, "our system . . . does not afford a remedy even for mental suffering which results from mere contumely and insult").

[38] *See id.* at 197 (positing that a "legal remedy for [a privacy] injury" would treat the "wound[ing of] feelings[] as a substantive cause of action").

[39] *See* Prosser, *supra* note 20, at 389 (examining over three hundred cases to find legal recognition of "four distinct kinds of invasion of four different interests of the plaintiff").

[40] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 97-101 (2004) [hereinafter SOLOVE, THE DIGITAL PERSON] (identifying the influence of "an architecture that structures power, a regulatory framework that governs how information is disseminated, collected and networked" on protecting privacy).

a person and more the creation of the risk that a person might be harmed in the future. They are akin, in many ways, to environmental harms or pollution. In the taxonomy, two kinds of architectural issues emerge most often. First is the enhancement of the risk that a harm will occur. Activities involving a person's information, for example, might create a greater risk of that person being victimized by identity theft or fraud. Such risk-enhancing activities increase the chances of the individual suffering dignitary harms as well as monetary or physical harms. Second, a particular activity can upset the balance of social or institutional power in undesirable ways. A particular individual may not be harmed directly, but this balance of power can affect that person's life. The classic example is law enforcement officials having too much power, which can alter the way people engage in their activities. People's behavior might be chilled, making them less likely to attend political rallies or criticize popular views. Surveillance can also have these effects. This kind of harm is often referred to as a "chilling effect."[41] Imbalances in power can also be risk enhancing, in that they increase the risk of abuses of power.

When we speak of these activities, we often focus on how they affect an individual's life. This does not mean that privacy is an individualistic right. Philosopher John Dewey astutely argued that individual rights need not be justified as the immutable possessions of individuals; instead, they are instrumental in light of "the contribution they make to the welfare of the community."[42] Employing a similar insight, several scholars contend that privacy is "constitutive" of society. Constitutive privacy understands privacy harms as extending beyond the "mental pain and distress" caused to particular individuals; privacy harms affect the nature of society and impede individual activities that contribute to the greater social good. Spiros Simitis recognizes that "privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone."[43] Robert Post contends that the tort of invasion of privacy "safe-

---

[41] *See, e.g.*, Laird v. Tatum, 408 U.S. 1, 1, 13 (1972) (confronting the alleged "chilling effect" that Army surveillance had on "lawful and peaceful civilian political activity").

[42] JOHN DEWEY, *Liberalism and Civil Liberties*, *in* 11 LATER WORKS 372, 373 (Jo Ann Boydston ed., S. Ill. Univ. Press 1987) (1936).

[43] Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 709 (1987). In analyzing the problems of federal legislative policymaking on privacy, Priscilla Regan demonstrates the need for understanding privacy in terms of its social benefits. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY, xiv (1995) ("[A]nalysis of con-

guards rules of civility that in some significant measure constitute both individuals and community."[44] The theory of constitutive privacy has been further developed by Julie Cohen and Paul Schwartz, who both argue that privacy is a constitutive element of a civil society.[45]

In the taxonomy that follows, there are four basic groups of harmful activities: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion. Each of these groups consists of different related subgroups of harmful activities.

I have arranged these groups around a model that begins with the data subject—the individual whose life is most directly affected by the activities classified in the taxonomy. From that individual, various entities (other people, businesses, and the government) collect information. The collection of this information itself can constitute a harmful activity. Not all information collection is harmful, but certain kinds of collection can be. Those that collect the data (the "data holders") then process it—they store it, combine it, manipulate it, search it, and use it. I label these activities as "information processing."[46] The next step is "information dissemination," in which the data holders transfer the information to others or release the information. The general progression from information collection to processing to dissemination is the data moving further away from the control of the individual. The last grouping of activities is "invasions," which involve impingements directly on the individual. Instead of the progression away from the individual, invasions progress toward the individual and do not necessarily involve information. The relationship between these different groupings is depicted in Figure 1 below.[47]

---

gressional policy making reveals that little attention was given to the possibility of a broader social importance of privacy.").

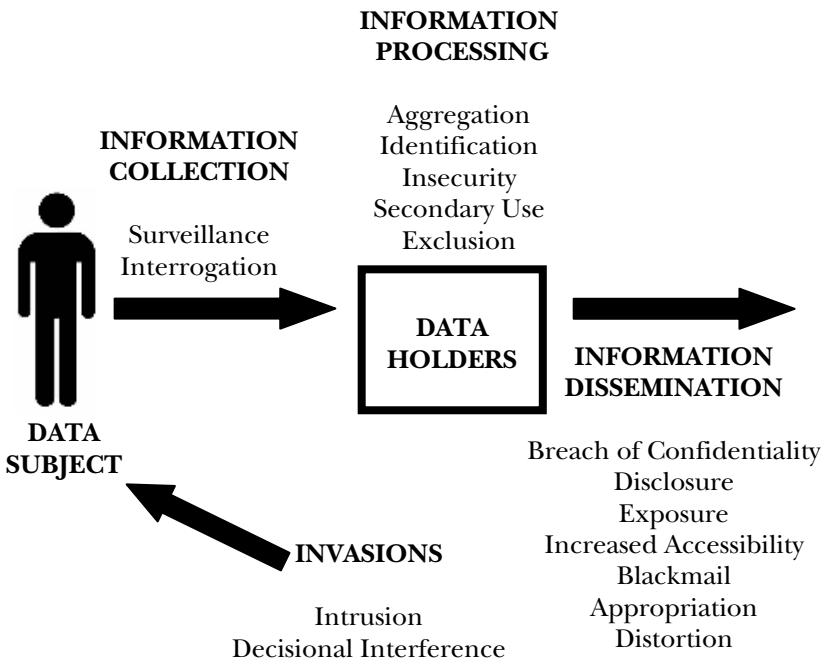
[44] Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 959 (1989).

[45] *See* Cohen, *supra* note 28, at 1427-28 ("Informational privacy, in short, is a constitutive element of a civil society in the broadest sense of the term."); Schwartz, *supra* note 18, at 1613 ("[I]nformation privacy is best conceived of as a constitutive element of civil society."); *see also* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 455 (1980) ("Privacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy.").

[46] I borrow the term "processing" from the European Union Data Protection Directive. *See* Council Directive 95/46, art. 2(b), 1995 O.J. (L 281) 31 (EC).

[47] I thank Peter Swire for suggesting and helping to develop this diagram.

Figure 1



The first group of activities that affect privacy involves information collection. *Surveillance* is the watching, listening to, or recording of an individual's activities. *Interrogation* consists of various forms of questioning or probing for information.

A second group of activities involves the way information is stored, manipulated, and used—what I refer to collectively as "information processing." *Aggregation* involves the combination of various pieces of data about a person. *Identification* is linking information to particular individuals. *Insecurity* involves carelessness in protecting stored information from leaks and improper access. *Secondary use* is the use of information collected for one purpose for a different purpose without the data subject's consent. *Exclusion* concerns the failure to allow the data subject to know about the data that others have about her and participate in its handling and use. These activities do not involve the gathering of data, since it has already been collected. Instead, these activities involve the way data is maintained and used.

The third group of activities involves the dissemination of information. *Breach of confidentiality* is breaking a promise to keep a person's information confidential. *Disclosure* involves the revelation of truthful information about a person that impacts the way others judge her character. *Exposure* involves revealing another's nudity, grief, or bodily functions. *Increased accessibility* is amplifying the accessibility of information. *Blackmail* is the threat to disclose personal information. *Appropriation* involves the use of the data subject's identity to serve the aims and interests of another. *Distortion* consists of the dissemination of false or misleading information about individuals. Information dissemination activities all involve the spreading or transfer of personal data or the threat to do so.

The fourth and final group of activities involves invasions into people's private affairs. Invasion, unlike the other groupings, need not involve personal information (although in numerous instances, it does). *Intrusion* concerns invasive acts that disturb one's tranquility or solitude. *Decisional interference* involves the government's incursion into the data subject's decisions regarding her private affairs.

A. *Information Collection*

Information collection creates disruption based on the process of data gathering. Even if no information is revealed publicly, information collection can create harm. I will identify two forms of information collection: (1) surveillance and (2) interrogation.

1. Surveillance

For a long time, surveillance has been viewed as problematic. The term "Peeping Tom" originates from a legend dating back to 1050. When Lady Godiva rode naked on a horse in the city of Coventry to protest taxes, a young man named Tom gawked at her, and he was punished by being blinded.[48] Today, many states have Peeping Tom laws. South Carolina, for example, criminalizes "peep[ing] through windows, doors, or other like places, on or about the premises of another, for the purpose of spying upon or invading the privacy of the

[48] CLAY CALVERT, VOYEUR NATION 36-38 (2000); Avishai Margalit, *Privacy in the Decent Society*, 68 SOC. RES. 255, 259 (2001). In another version of the story, Tom is not blinded by others, but inexplicably struck blind upon looking at her after Lady Godiva asked the townspeople not to look. BBC, Beyond the Broadcast, Making History: Lady Godiva of Coventry, http://www.bbc.co.uk/education/beyond/factsheets/makhist/makhist6_prog9d.shtml (last visited Jan. 21, 2006).

persons spied upon and any other conduct of a similar nature, that tends to invade the privacy of others."[49] Some states prohibit two-way mirrors in certain areas.[50]

As with visual surveillance, audio surveillance has long been viewed as troubling. William Blackstone noted that eavesdropping was a common law crime, and defined it as "listen[ing] under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales."[51] These attitudes persisted after the emergence of electronic eavesdropping. As early as 1862, California prohibited the interception of telegraph communications.[52] Soon after telephone wiretapping began in the 1890s, several states prohibited it, such as California in 1905.[53] By 1928, over half the states had made wiretapping a crime.[54] Justice Holmes referred to wiretapping as a "dirty business,"[55] and Justice Frankfurter called it "odious."[56] When the Supreme Court held in the 1928 case *Olmstead v. United States* that the Fourth Amendment did not protect against wiretapping,[57] Congress responded six years later by making wiretapping a federal crime.[58] In 1967, the Supreme Court changed its position on wiretapping, overruling *Olmstead* in *Katz v. United States*.[59] One year later, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968, Title III of which provided com-

---

[49] S.C. CODE ANN. § 16-17-470(A) (2003); *see also* GA. CODE ANN. § 16-11-61 (2003) (criminalizing being a "peeping Tom" when "on or about the premises of another"); LA. REV. STAT. ANN. § 14:284 (2004) (defining "Peeping Tom" and setting forth the penalty); N.C. GEN. STAT. § 14-202 (Supp. 2004) (criminalizing peeping as a Class 1 misdemeanor); VA. CODE ANN. § 18.2-130 (2004) (criminalizing peeping or spying into a "dwelling or enclosure").

[50] For example, in California, "[a]ny person who installs or who maintains . . . any two-way mirror permitting observation of any restroom, toilet, bathroom, washroom, shower, locker room, fitting room, motel room, or hotel room is guilty of a misdemeanor." CAL. PENAL CODE § 653n (West 1988).

[51] 4 WILLIAM BLACKSTONE, COMMENTARIES *169.

[52] SAMUEL DASH ET AL., THE EAVESDROPPERS 25-26 (1959).

[53] *Id.* at 8, 25.

[54] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 841 (2004) (citing Berger v. New York, 388 U.S. 41, 45 (1967)).

[55] Olmstead v. United States, 277 U.S. 438, 470 (1928) (Holmes, J., dissenting).

[56] On Lee v. United States, 343 U.S. 747, 758-59 (1952) (Frankfurter, J., dissenting).

[57] 277 U.S. at 466.

[58] *See* Federal Communications Act of 1934, Pub. L. No. 90-351, § 2520, 48 Stat. 1103 (codified as amended at 47 U.S.C. § 605 (2000)).

[59] 389 U.S. 347, 353 (1967).

prehensive protection against wiretapping.[60] Title III required law enforcement officials to obtain a warrant before wiretapping and criminalized wiretaps by private parties.[61] Congress amended Title III in 1986 with the Electronic Communications Privacy Act (ECPA), expanding Title III's protections from wiretapping to additional forms of electronic surveillance.[62]

What is the harm if people or the government watch or listen to us? Certainly, we all watch or listen, even when others may not want us to, and we often do not view this as problematic. However, when done in a certain manner—such as continuous monitoring—surveillance has problematic effects. For example, people expect to be looked at when they ride the bus or subway, but persistent gawking can create feelings of anxiety and discomfort.

Not only can direct awareness of surveillance make a person feel extremely uncomfortable, but it can also cause that person to alter her behavior. Surveillance can lead to self-censorship and inhibition.[63] Because of its inhibitory effects, surveillance is a tool of social control, enhancing the power of social norms, which work more effectively when people are being observed by others in the community.[64] John Gilliom observes: "Surveillance of human behavior is in place to control human behavior, whether by limiting access to programs or institutions, monitoring and affecting behavior within those arenas, or otherwise enforcing rules and norms by observing and recording acts of compliance and deviance."[65] This aspect of surveillance does not automatically make it harmful, though, since social control can be

---

[60] Pub. L. No. 90-351, ch. 119, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2522 (2000)).

[61] 82 Stat. 213-14 (codified as amended at 18 U.S.C. § 2511 (2000)).

[62] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2520, 2701-2711, 3121-3127 (2000)) (expanding Titles I-III to protect "wire, oral, or electronic communications").

[63] *See* Kang, *supra* note 19, at 1193, 1260 ("Simply put, surveillance leads to self-censorship."); Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 473 (1999) ("If I know I am under surveillance, I might . . . restrict my activities, so that nothing embarrassing or otherwise harmful could be detected.").

[64] As Judge Posner notes, "norms are more effective when people are under the observation of their peers." RICHARD A. POSNER, THE PROBLEMATICS OF MORAL AND LEGAL THEORY 75 (1999); *see also* JAMES B. RULE, PRIVATE LIVES AND PUBLIC SURVEILLANCE 28 (1974) (finding both large-scale and less formal surveillance to be helpful to a government "or any other agency seeking to obtain compliance from a mass clientele in a large-scale social setting").

[65] JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY 3 (2001).

beneficial and every society must exercise a sizeable degree of social control. For example, surveillance can serve as a deterrent to crime. Many people desire the discipline and control surveillance can bring. Jeff Rosen observes that Britain's closed circuit television (CCTV)—a network of over four million public surveillance cameras—is widely perceived as "a friendly eye in the sky, not Big Brother but a kindly and watchful uncle or aunt."[66]

Too much social control, however, can adversely impact freedom, creativity, and self-development. According to Julie Cohen, "pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream."[67] Monitoring constrains the "acceptable spectrum of belief and behavior," and it results in "a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines."[68] Surveillance thus "threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it."[69] Similarly, Paul Schwartz argues that surveillance inhibits freedom of choice, impinging upon self-determination.[70]

In many instances, people are not directly aware that they are being observed. Does covert surveillance cause a problem? Under one view, surveillance is a prima facie wrong, whether overt or covert, for it demonstrates a lack of respect for its subject as an autonomous person. Philosopher Stanley Benn explains that overt surveillance does so by threatening its target's "consciousness of pure freedom as subject, as originator and chooser."[71] As Benn contends, "[f]inding oneself an object of scrutiny, as the focus of another's attention, brings one to a new consciousness of oneself, as something seen through another's eyes."[72] Turning to covert observation, Benn explains that it "is objectionable because it deliberately deceives a person about his

---

[66] JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 36 (2004).

[67] Cohen, *supra* note 28, at 1426.

[68] *Id.*

[69] *Id.*

[70] *See* Schwartz, *supra* note 18, at 1656 ("[P]erfected surveillance of naked thought's digital expression short-circuits the individual's own process of decisionmaking.").

[71] Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* NOMOS XIII: PRIVACY 1, 7 (J. Roland Pennock & John W. Chapman eds., 1971).

[72] *Id.*

world, thwarting, for reasons that *cannot* be his reasons, his attempts to make a rational choice."[73]

Although concealed spying is certainly deceptive, Benn's argument is unconvincing. It is the awareness that one is being watched that affects one's freedom, and Benn fails to explain why covert surveillance has any palpable effect on a person's welfare or activities. A more compelling reason why covert surveillance is problematic is that it can have a chilling effect on behavior. In fact, there can be an even greater chilling effect when people are generally aware of the *possibility* of surveillance, but are never sure if they are being watched at any particular moment. This phenomenon is known as the Panoptic effect, based on Jeremy Bentham's 1791 architectural design for a prison called the Panopticon.[74] The prison was set up with the inmates' cells arrayed around a central observation tower. Most importantly, the guards could see each prisoner from the tower, but the prisoners could not see the guards from their cells.[75] In Michel Foucault's words, the cells were akin to "small theatres, in which each actor is alone, perfectly individualized and constantly visible."[76] The prisoner's "only rational option" was to conform with the prison's rules because, at any moment, it was possible that they were being watched.[77] Thus, awareness of the possibility of surveillance can be just as inhibitory as actual surveillance.

One might attempt to imagine surveillance so covert that its subjects are completely unaware of even the possibility of being observed. While such well-concealed surveillance might eliminate the potential for any discomfort or chilling effect, it would still enable the watchers to gather a substantial degree of information about people, creating an architectural problem.[78] Surveillance is a sweeping form of investigatory power. It extends beyond a search, for it records behavior, social interaction, and potentially everything that a person says and does. Rather than targeting specific information, surveillance can ensnare a significant amount of data beyond any originally sought. If watched long enough, a person might be caught in some form of illegal or im-

---

[73] *Id.* at 10.

[74] DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY 62-67 (1994).

[75] *Id.* at 62-63.

[76] MICHEL FOUCAULT, DISCIPLINE AND PUNISH 200 (Alan Sheridan trans., Vintage Books, 2d ed. 1995) (1977).

[77] LYON, *supra* note 74, at 63.

[78] *See supra* note 40 and accompanying text.

moral activity, and this information could then be used to discredit or blackmail her. A prime example is the FBI's extensive wiretapping of Martin Luther King, Jr., widely believed to have been initiated in order to expose King's alleged communist ties. Though the surveillance failed to turn up any evidence of such ties, it did reveal King's extramarital affairs. The FBI then attempted to blackmail King with the information, and FBI officials leaked it in order to discredit King.[79]

The law addresses surveillance, but does so by focusing on where surveillance takes place rather than on its problematic effects. The law often recognizes surveillance as a harm in private places but rarely in public places. In Fourth Amendment law, courts frequently conclude that surveillance in private places implicates a reasonable expectation of privacy whereas surveillance in public places does not. In *Kyllo v. United States*, the Court concluded that the Fourth Amendment required a warrant in order to use a thermal-imaging device to detect heat patterns emanating from a person's home.[80] The Court's holding relied heavily on the fact that, though conducted outside the petitioner's home, the surveillance was capturing information about activities within it: "We have said that the Fourth Amendment draws a firm line at the entrance of the house."[81]

When surveillance occurs in a public place, however, the Court has refused to recognize a reasonable expectation of privacy. In *Florida v. Riley*, the police flew over the defendant's greenhouse in a helicopter at four hundred feet and peered down through a few missing roof panels to observe that he was growing marijuana.[82] The Court concluded that the defendant lacked a reasonable expectation of privacy: "As a general proposition, the police may see what may be seen from a public vantage point where [they have] a right to be."[83] In *Dow Chemical Co. v. United States*, the Court held that the government could not only fly over the petitioner's property and observe it with the naked eye, but could also use a powerful aerial mapping camera that en-

---

[79] SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 185. For a more extensive account of King's experience with the FBI, see DAVID J. GARROW, THE FBI AND MARTIN LUTHER KING, JR. (1981).

[80] 533 U.S. 27, 40 (2001).

[81] *Id.* (internal quotation marks omitted); *see also* Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS. 125, 144 (2002) ("Central to the Court's reasoning was that the thermal imager revealed information concerning activities *inside the home*.").

[82] 488 U.S. 445, 448-49 (1989).

[83] *Id.* at 449 (alteration in original) (internal quotation marks omitted).

abled the identification of objects as small as one-half inch in diameter.[84]

The contrast between the law's approach to surveillance in private and in public is most evident in a pair of Supreme Court cases involving location-tracking devices. In *United States v. Karo*, the Court concluded that a tracking device that monitored a person's movements within his home implicated that person's reasonable expectation of privacy.[85] In contrast, in *United States v. Knotts*, the police placed a tracking device in a can of chloroform, which the defendant then purchased and placed in his car.[86] Using the device, the police tracked the location of the defendant's vehicle.[87] According to the Court, the surveillance "amounted principally to the following of an automobile on public streets and highways."[88] The Court concluded that the Fourth Amendment did not apply because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[89] Therefore, the Court has concluded that while the Fourth Amendment protects against surveillance in private places such as one's home, the Amendment has little applicability to surveillance in public places.[90] This understanding of privacy stems from what I call the "secrecy paradigm."[91] Under the secrecy paradigm, privacy is tantamount to complete secrecy, and a privacy violation occurs when concealed data is revealed to others. If the information is not previously hidden, then no privacy interest is implicated by the collection or dissemination of the information. In many areas of law, this narrow view of privacy has limited the recognition of privacy violations.

Tort law is generally consistent with this approach. Courts have applied the tort of intrusion upon seclusion, which protects against

---

[84] 476 U.S. 227, 238-39 (1986).

[85] 468 U.S. 705, 714 (1984).

[86] 460 U.S. 276, 277 (1983).

[87] *Id.*

[88] *Id.*

[89] *Id.* at 281.

[90] *See, e.g.*, Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1357 (2004) ("[C]ontemporary Fourth Amendment jurisprudence differentiates pervasive video surveillance from more familiar mass suspicionless searches in one crucial respect: by holding that it is not a 'search' at all."); *cf.* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 233 (2002) ("Meaningful legal strictures on government use of public surveillance cameras in Great Britain, Canada, and the United States are non-existent.").

[91] SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 42-44.

intrusion "upon the solitude or seclusion of another or his private affairs or concerns,"[92] to surveillance of private places. In *Hamberger v. Eastman*, for example, the court concluded that a couple had a valid intrusion claim against their landlord for his installation of a hidden recording device in their bedroom.[93] In contrast, plaintiffs bringing claims involving surveillance in public have generally not been successful.[94]

In some cases, however, courts have recognized a harm in public surveillance. For example, in *Nader v. General Motors Corp.*, Ralph Nader charged that General Motors's automobiles were unsafe.[95] General Motors undertook a massive investigation seeking information discrediting Nader. Among other things, General Motors wiretapped his telephone and placed him under extensive surveillance while in public.[96] The court recognized that certain kinds of public surveillance might amount to an invasion of privacy; although observation "in a public place does not amount to an invasion of . . . privacy," in certain instances, "surveillance may be so 'overzealous' as to render it actionable."[97] The court noted: "A person does not automatically make public everything he does merely by being in a public place, and the mere fact that Nader was in a bank did not give anyone the right to try to discover the amount of money he was withdrawing."[98] The majority reasoned that extensive public surveillance can reveal hidden details that would not ordinarily be observed by others.[99] The court's analysis, however, focused more on the harm of disclosure than on that of surveillance; pervasive surveillance could reveal details people ordinarily conceal, and thus result in the discov-

---

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

[93] 206 A.2d 239, 241-42 (N.H. 1964); *see also* Wolfson v. Lewis, 924 F. Supp. 1413, 1431 (E.D. Pa. 1996) (finding media surveillance of a couple's activities in their home to be actionable under intrusion tort); Rhodes v. Graham, 37 S.W.2d 46, 47 (Ky. 1931) (holding that wiretapping a person's phone gives rise to a tort action because it violates his right "to the privacy of his home as against the unwarranted invasion of others").

[94] *See, e.g.*, Furman v. Sheppard, 744 A.2d 583, 586 (Md. Ct. Spec. App. 2000) (holding that the defendant was not liable under intrusion tort for trespassing into a private club to engage in video surveillance of the plaintiff because the club was not a secluded place); Forster v. Manchester, 189 A.2d 147, 149-50 (Pa. 1963) (finding no intrusion liability when a private investigator followed and filmed the plaintiff because the surveillance was conducted in public).

[95] 225 N.E.2d 765, 767 (N.Y. 1970).

[96] *Id.*

[97] *Id.* at 771.

[98] *Id.*

[99] *Id.* at 769.

ery of secrets.[100] The court did not recognize the surveillance as a harm itself—only surveillance that destroyed secrecy represented an actionable harm.[101]

Therefore, although the law often focuses on whether surveillance occurs in a public or private place, surveillance is harmful in all settings, not just private ones.[102] Surveillance in public can certainly cause uneasiness, as illustrated by the example of being stared at continuously in public. As Alan Westin observes: "Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas."[103] Moreover, public surveillance can have chilling effects that make people less likely to associate with certain groups, attend rallies, or speak at meetings.[104] Espousing radical beliefs and doing unconventional things takes tremendous courage; the attentive gaze, especially the government's, can make these acts seem all the more daring and their potential risks all the more inhibitory. Thus, the dignitary harms and architectural problems of surveillance can occur both in public and private places. The law, however, tends to focus more on secrecy than on the particular problems and harms caused by surveillance.

2. Interrogation

The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[105] The Amendment creates a "privilege against self-incrimination," and it prevents the government from compelling individuals to testify against themselves.[106] The privilege has been justified as protecting

---

[100] *Id.* at 768-69.

[101] *Id.* at 771 ("On the other hand, if the plaintiff acted in such a way as to reveal that fact to any casual observer, then, it may not be said that the appellant intruded into his private sphere.").

[102] *See* ABA CRIMINAL JUSTICE SECTION'S STANDARDS COMM., ABA CRIMINAL JUSTICE STANDARDS ON ELECTRONIC SURVEILLANCE RELATING TO TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE § 2-6.1(d) to (g) (Draft 3d ed. 1997) (recommending that the law begin to address the harms of public surveillance).

[103] WESTIN, *supra* note 19, at 31.

[104] As Justice Douglas observed in another case: "Monitoring, if prevalent, certainly kills free discourse and spontaneous utterances." United States v. White, 401 U.S. 745, 762 (1971) (Douglas, J., dissenting).

[105] U.S. CONST. amend. V.

[106] DAVID M. O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY 92-93 (1979) (emphasis omitted).

against "[t]he essential and inherent cruelty of compelling a man to expose his own guilt,"[107] as "a safeguard of conscience and human dignity,"[108] and as promoting "respect for personal integrity."[109]

What is so inhumane about having to answer the government's questions about one's criminal acts? Why do we want to protect a potentially guilty person from having to divulge her criminal activities?

A different, less coercive form of interrogation occurs when others or the government ask questions for purposes other than criminal prosecution. In the late nineteenth century, there was a loud public outcry when the U.S. census began including more and more questions relating to personal affairs, such as marital status, literacy, property ownership, health, and finances.[110] In the 1870s, an editorial in *The New York Times*, as well as editorials in other papers, decried the "inquisitorial" nature of the census.[111] A poem in *The New York Sun* in 1890 humorously criticized the census:

> I am a census inquisitor.
> I travel about from door to door,
> From house to house, from store to store,
> With pencil and paper and power galore.
> I do as I like and ask what I please.
> Down before me you must get on your knees;
> So open your books, hand over your keys,
> And tell me about your chronic disease.[112]

Why was there such an outcry? When asked a probing question that people find unwarranted, a frequent response is a snippy reply: "None of your business!" Why do such questions evoke such a response? Why do people take offense even at being asked certain questions—let alone being compelled to answer them?

Understood broadly, these examples all involve a similar practice—what I call "interrogation." Interrogation is the pressuring of individuals to divulge information. Interrogation has many benefits; it is useful for ferreting out information that others want to know.

---

[107] Brown v. Walker, 161 U.S. 591, 637 (1896) (Field, J., dissenting).

[108] Ullmann v. United States, 350 U.S. 422, 445 (1956) (Douglas, J., dissenting).

[109] Charles Fried, *Privacy*, 77 YALE L.J. 475, 488 (1968).

[110] *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1401 (2001).

[111] ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 62 (2000).

[112] *Id.* at 63.

However, interrogation can create harm. Part of this harm arises from the degree of coerciveness involved. The Fifth Amendment privilege protects against highly coercive interrogation about matters with enormous personal stakes for the examined subject.[113] However, for interrogation generally, the compulsion need not be direct; nor must it rise to the level of outright coercion. Compulsion can consist of the fear of not getting a job or of social opprobrium. People take offense when others ask an unduly probing question—even if there is no compulsion to answer. One explanation may be that people still feel some degree of compulsion because not answering might create the impression that they have something to hide. This is why, I believe, there are social norms against asking excessively probing or prying questions: they make the person being questioned feel uncomfortable. Interrogation forces people to be concerned about how they will explain themselves or how their refusal to answer will appear to others.

Interrogation resembles intrusion in its invasiveness, for interrogation is a probing, a form of searching. Like disclosure, interrogation often involves the divulging of concealed information; unlike disclosure, interrogation can create discomfort even if the information is barely disseminated. To some degree, surveillance resembles interrogation, for both involve the involuntary gathering of information. Interrogation, however, occurs with the conscious awareness of the subject; surveillance can be clandestine.

Historically, interrogation has been employed to impinge upon freedom of association and belief. During the McCarthy era in the 1950s, the House Un-American Activities Committee (HUAC) employed interrogation to attack Communists and inhibit their association and expression of political beliefs.[114] Dissenting in *Barenblatt v. United States*, in which the Court upheld the Committee's power to force a witness to answer questions about Communist ties,[115] Justices Black, Warren and Douglas argued that the interrogation's harm did not affect the witness alone.[116] They spoke of interrogation impeding "the interest of *the people as a whole* in being able to join organizations,

---

[113] *See, e.g.*, Miranda v. Arizona, 384 U.S. 436, 467 (1966) (explaining the Fifth Amendment protections against self-incrimination in the context of custodial interrogation).

[114] ELLEN SCHRECKER, MANY ARE THE CRIMES: MCCARTHYISM IN AMERICA 369-70 (1998).

[115] 360 U.S. 109, 127, 134 (1959).

[116] *Id.* at 144 (Black, J., dissenting).

advocate causes and make political 'mistakes' without later being subjected to governmental penalties for having dared to think for themselves."[117]

Another aspect of the power of interrogation is its potential for resulting in distortion. The interrogator possesses extraordinary control over what information is elicited, how it is interpreted, and the impressions created by its revelations. A skillful interrogator can orchestrate a dialogue that creates impressions and inferences that she wants to elicit. In cross-examination, a skilled attorney can carefully manipulate what a witness says and can intimidate a witness into coming across less favorably. Thus, one of the rationales justifying the privilege against self-incrimination is that it protects accuracy.[118] Even in the absence of deliberate manipulation, the interrogation process can be distorting. "The interrogat[ion]," observes Peter Brooks, "seeks to pattern the unfolding narrative according to a preconceived story."[119] Interrogation can be distorting because information is elicited by another, often without an interest in learning the whole story. In questionnaires and standardized forms, for example, distortion creeps in because the questions often do not ask for the entire story or are phrased in certain ways that yield deceptive results.

Beyond the Fifth Amendment, there are numerous legal protections against interrogation. The First Amendment prevents government questioning about one's political associations. In *Shelton v. Tucker*, the Court applied strict scrutiny and struck down a law requiring public teachers to list all organizations to which they belong or contribute.[120] Later, in *Baird v. State Bar of Arizona*, the Court held that a state may not ask questions solely to gain information about a person's political views or associations.[121] According to the Court:

---

[117] *Id.* (emphasis added).

[118] As Wigmore noted: "The simple and peaceful process of questioning breeds a readiness to resort to bullying and to physical force and torture." 8 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2251 n.1(c) (John T. McNaughton ed., 4th ed. 1961).

[119] PETER BROOKS, TROUBLING CONFESSIONS: SPEAKING GUILT IN LAW AND LITERATURE 40 (2000). The interrogation of Dimitri Karamazov in Fyodor Dostoevsky's *The Brothers Karamazov* is an excellent literary example of how interrogation distorts the truth even when the interrogators bear no deliberate motivation to distort. *See* RICHARD H. WEISBERG, THE FAILURE OF THE WORD 55-58 (1984) (commenting on "Dostoevsk[y]'s belief that the legal investigator, like the novelist himself, is motivated by an essentially personalized vision of reality").

[120] 364 U.S. 479, 488-90 (1960).

[121] 401 U.S. 1, 6-7 (1971). If the government has other purposes for asking such information, however, questions about political views and organizations are permissi-

"[W]hen a State attempts to make inquiries about a person's beliefs or associations, its power is limited by the First Amendment. Broad and sweeping state inquiries into these protected areas, as Arizona has engaged in here, discourage citizens from exercising rights protected by the Constitution."[122]

Rape shield laws restrict the questioning of rape victims in court.[123] The Americans with Disabilities Act of 1990 limits certain employer inquiries about employee disabilities.[124] Many states prohibit employers from questioning employees or applicants about certain matters. For example, Wisconsin forbids employers from requiring employees or applicants to undergo HIV testing.[125] Massachusetts prohibits employers from asking about arrests not leading to conviction, misdemeanor convictions, or any prior commitment to mental health treatment facilities.[126] Several states restrict employers from requiring employees or applicants to undergo genetic testing.[127] Evidentiary privileges protect communications between attorneys and clients, priests and penitents, and doctors and patients.[128] Privileges

---

ble. *See* Law Students Civil Rights Research Council, Inc. v. Wadmond, 401 U.S. 154, 165-66 (1971) (remarking that questions about membership and intent to further a subversive organization's illegal aims were constitutionally proper); Barenblatt v. United States, 360 U.S. 109, 127-28 (1959) (holding that a person could be compelled to disclose before the House Un-American Activities Committee whether he was a member of the Communist Party because questions were related to a "valid legislative purpose").

[122] *Baird*, 401 U.S. at 6.

[123] *See* Harriet R. Galvin, *Shielding Rape Victims in the State and Federal Courts: A Proposal for the Second Decade*, 70 MINN. L. REV. 763, 765-66 (1986) (discussing how rape shield laws reversed the common law doctrine that allowed a defendant to inquire into the complainant's tendency to engage in extramarital sexual relations).

[124] *See* 42 U.S.C. § 12112(d)(2) (2000) (limiting the legality of inquiries during the pre-employment period); *id.* § 12112(d)(4) (prohibiting inquiries during the employment period). Drug testing is not considered a "medical examination" under the ADA. *Id.* § 12114(d)(1).

[125] WIS. STAT. ANN. § 103.15(2) (West 2002).

[126] MASS. GEN. LAWS ANN. ch. 151B, § 4(9), (9A) (LexisNexis 1999).

[127] *See, e.g.*, CAL. GOV'T CODE § 12940(o) (West 2005); CONN. GEN. STAT. ANN. § 46a-60(11)(A) (West 2004); DEL. CODE ANN. tit. 19, § 711(e) (Supp. 2004); N.Y. EXEC. LAW § 296.19(a)(1) (McKinney 2004).

[128] *See, e.g.*, ARIZ. REV. STAT. ANN. § 12-2235 (2005) (privileging, in civil actions, any patient communication to a physician or surgeon regarding "any physical or mental disease or disorder or supposed physical or mental disease or disorder or as to any such knowledge obtained by personal examination of the patient"); CAL. EVID. CODE § 954 (West 1995) ("[T]he client . . . has a privilege to refuse to disclose, and to prevent another from disclosing, a confidential communication between client and lawyer . . . ."); 735 ILL. COMP. STAT. ANN. 5/8-803 (West 2005) (rendering privileged any

do not guard against the questioning of the individual about her personal information; rather, they protect against the questioning of others about it. As Catherine Ross contends, privileges protect against "forced betrayal."[129]

Although the law protects against interrogation, it does so in a complicated and unsystematic way. The Fifth Amendment's protection against interrogation is very limited. The Fifth Amendment certainly does not protect the information itself; if the same facts can be produced at trial via other witnesses or evidence, they are not prohibited. The Fifth Amendment is therefore concerned only partly with the type of information involved—its applicability turns on compelled self-disclosure. However, as William Stuntz observes, under current Fifth Amendment law:

> As long as use immunity is granted, the government is free to compel even the most damning and private disclosures. . . . If the privilege were sensibly designed to protect privacy, . . . its application would turn on the *nature* of the disclosure the government wished to require, and yet settled fifth amendment law focuses on the criminal *consequences* of disclosure.[130]

Incriminating information may thus be compelled even under the Fifth Amendment if there are no criminal consequences—even if the compulsion would cause a person great disgrace.[131] In *Ullmann v. United States,* for example, a witness granted immunity to testify as to his activities in the Communist Party contended that he would not only suffer disgrace, but would suffer severe social sanctions as a result, including losing his job and friends , and being blacklisted from future employment.[132] The Court rejected the witness's argument because no criminal sanctions would be imposed as a result of his testifying.[133] In dissent, Justice Douglas argued that the "Fifth Amendment was designed to protect the accused against infamy as well as against

---

"confession or admission" made to an accredited practitioner of a religious denomination in her official capacity).

[129] Catherine J. Ross, *Implementing Constitutional Rights for Juveniles: The Parent-Child Privilege in Context*, 14 STAN. L. & POL'Y REV. 85, 86 (2003).

[130] William J. Stuntz, *Self-Incrimination and Excuse*, 88 COLUM. L. REV. 1227, 1234 (1988) (footnotes omitted).

[131] *See* Brown v. Walker, 161 U.S. 591, 605-06 (1896) ("The design of the constitutional privilege [against self-incrimination] is not to aid the witness in vindicating his character, but to protect him against being compelled to furnish evidence to convict him of a criminal charge.").

[132] 350 U.S. 422, 430 (1956).

[133] *Id.* at 439.

prosecution," and that the "curse of infamy" could be as damaging as criminal punishment.[134] Nevertheless, Douglas's view has not been accepted in Fifth Amendment doctrine. It remains unclear what interests the Fifth Amendment protects. As Stuntz observes: "It is probably fair to say that most people familiar with the doctrine surrounding the privilege against self-incrimination believe that it cannot be squared with any rational theory."[135]

Evidentiary privileges, like the Fifth Amendment, are also quite narrow in scope. Despite strong public disapproval of forcing parents and children to testify against each other, the majority of courts have rejected a parent-child privilege.[136] Still, in the words of one court, "forcing a mother and father to reveal their child's alleged misdeeds . . . is shocking to our sense of decency, fairness and propriety."[137]

Privacy law's theory of interrogation is not only incoherent, it is nearly nonexistent. Despite recognizing the harms and problems of interrogation—compulsion, divulgence of private information, and forced betrayal—the law only addresses them in limited situations.

B. *Information Processing*

Information processing refers to the use, storage, and manipulation of data that has been collected. Information processing does not involve the collection of data; rather, it concerns how already-collected data is handled. I will discuss five forms of information proc-

---

[134] *Id.* at 450, 452 (Douglas, J., dissenting).

[135] Stuntz, *supra* note 130, at 1228.

[136] *See In re* Grand Jury, 103 F.3d 1140, 1146 (3d Cir. 1997) ("The overwhelming majority of all courts—federal or state—have rejected such a privilege.").

[137] *In re* A & M, 403 N.Y.S.2d 375, 380 (App. Div. 1978). When Monica Lewinsky's mother was subpoenaed to testify against her by Independent Counsel Ken Starr in his investigation of President Bill Clinton, there was an enormous public outcry. *See* Ruth Marcus, *To Some in the Law, Starr's Tactics Show a Lack of Restraint*, WASH. POST, Feb. 13, 1998, at A1 (providing reactions from prosecutors who believed Starr's tactics were unwarranted). Critics have likened the tactic of having parents and children testify about each other to some of the infamous horrors of totalitarian societies, such as Nazi Germany, where the government sought to make family members divulge information about each other. *See, e.g.*, J. Tyson Covey, *Making Form Follow Function: Considerations in Creating and Applying a Statutory Parent-Child Privilege*, 1990 U. ILL. L. REV. 879, 890 (postulating that recognition of some form of a parent-child privilege would help to prevent the state from forcing children and parents into a troubling predicament); Wendy Meredith Watts, *The Parent-Child Privileges: Hardly a New or Revolutionary Concept*, 28 WM. & MARY L. REV. 583, 590-94 (1987) (noting that parent-child privileges are not recognized in despotic regimes).

essing: (1) aggregation, (2) identification, (3) insecurity, (4) secondary use, and (5) exclusion.

Processing involves various ways of connecting data together and linking it to the people to whom it pertains. Even though it can involve the transmission of data, processing diverges from dissemination because the data transfer does not involve the disclosure of the information to the public—or even to another person. Rather, data is often transferred between various record systems and consolidated with other data. Processing diverges from information collection because processing creates problems through the consolidation and use of the information, not through the means by which it is gathered.

1. Aggregation

The rising use of computers in the 1960s raised public concern about privacy.[138] Commentators devoted significant attention to the issue,[139] and privacy became an important topic on Congress's agenda.[140] Significant concern was devoted to the data maintained by the federal government. In 1965, a group of academics led by professor Richard Ruggles criticized the fact that the government's data systems were decentralized and recommended consolidation.[141] The Bureau of the Budget (now called the Office of Management and Budget) supported the idea and suggested the creation of a Federal

---

[138] REGAN, *supra* note 43, at 82.

[139] *See, e.g.*, MYRON BRENTON, THE PRIVACY INVADERS 13 (1964) (discussing how life in the 1960s brings with it some compulsory encroachments on privacy, but that "'reasonable' encroachments are fast becoming unreasonable . . . invasions . . . tending to make intrusion a way of everyday life"(emphasis omitted)); MILLER, *supra* note 5, at ix-x (discussing "the profound effect computer technology is certain to have on numerous facets of the law" including individual privacy); VANCE PACKARD, THE NAKED SOCIETY 12 (1964) ("Today it is increasingly assumed that the past and present of all of us . . . must be an open book; and that all such information about us can be not only put in files but merchandised freely."); WESTIN, *supra* note 19, at 3 (arguing that society needs to "move from public awareness of the problem to a sensitive discussion of what can be done to protect privacy in an age when so many forces of science [and] technology . . . press against it from all sides"); Kenneth L. Karst, *"The Files": Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROBS. 342, 343 (1966) (identifying two problems arising from the maintenance and usage of computerized personal data files—"access and accuracy" of information—which "raise divergent questions for the legal system"); Symposium, *Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211-45 (1968) (exploring the possibility and danger of National Data Banks, including personal privacy implications).

[140] *See* REGAN, *supra* note 43, at 82 (reporting that Congress held many hearings on the issue in the late 1960s and early 1970s).

[141] SMITH, *supra* note 111, at 309.

Data Center.[142] The plan was quickly attacked in Congress and scrapped.[143] In 1974, John Holt at the General Services Administration proposed the creation of FEDNET, a plan to link together all computer systems maintained by the federal government.[144] Vice President Ford immediately halted the plan and demoted Holt.[145]

What was the concern? The data was already in the record systems of government agencies. Why was it a problem for the government to combine it into one gigantic database?

The problem is one that I have called "aggregation."[146] Aggregation is the gathering together of information about a person. A piece of information here or there is not very telling. But when combined together, bits and pieces of data begin to form a portrait of a person. The whole becomes greater than the parts.[147] This occurs because combining information creates synergies. When analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected.

Aggregating information is certainly not a new activity. It was always possible to combine various pieces of personal information, to put two and two together to learn something new about a person. But aggregation's power and scope are different in the Information Age; the data gathered about people is significantly more extensive, the process of combining it is much easier, and the computer technologies to analyze it are more sophisticated and powerful.

Combining data and analyzing it certainly can be put to beneficial uses. Amazon.com, for example, uses aggregated data about a person's book-buying history to recommend other books that the person might find of interest. Credit reporting allows creditors to assess people's financial reputations in a world where first-hand experience of the financial condition and trustworthiness of individuals is often lack-

---

[142] *Id.* at 310-11. *But cf.* Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400, 412 (1968) (criticizing the congressional task force for undertaking "only a surface treatment" of the privacy issue and arguing that "Congress should give very careful consideration to essential legal and technological safeguards for the privacy interest").

[143] SMITH, *supra* note 111, at 311.

[144] *Id.*

[145] *Id.*

[146] SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 44-47.

[147] *See* Cohen, *supra* note 28, at 1398 ("A comprehensive collection of data about an individual is vastly more than the sum of its parts.").

ing.[148] These developments make sense in a world where there are billions of people and word-of-mouth is insufficient to assess reputation.

Alongside these benefits, however, aggregation can cause dignitary harms because of how it unsettles expectations. People expect certain limits on what is known about them and on what others will find out. Aggregation upsets these expectations, because it involves the combination of data in new, potentially unanticipated ways to reveal facts about a person that are not readily known. People give out bits of information in different settings, only revealing a small part of themselves in each context. Indeed, people selectively spread around small pieces of data throughout most of their daily activities, and they have the expectation that in each disclosure, they are revealing relatively little about themselves. When these pieces are consolidated together, however, the aggregator acquires much greater knowledge about the person's life.

Like surveillance, aggregation is a way to acquire information about people. It reveals facts about data subjects in ways far beyond anything they expected when they gave out the data. However, aggregation is a less direct form of data acquisition than surveillance, for it occurs through processing data already gathered from individuals.

Aggregation can also lead to architectural problems; it can increase the power that others have over individuals. The dossier created by aggregating a person's data is often used as a way to judge her. Aggregations of data, such as credit reports, are used to evaluate data about a person's financial reputation and then make decisions that profoundly affect a person's life, including whether she gets a loan, a lease, or a mortgage. Elsewhere, I have discussed the multitude of ways that the compilation of an individual's data—what I call the "digital person"—is being used to make important decisions about an individual. The digital person in digital space increasingly is affecting the flesh-and-blood individual in realspace.[149]

Although making decisions based on aggregated data is efficient, it also creates problems. Data compilations are often both telling and incomplete. They reveal facets of our lives, but the data is often re-

---

[148] *See* STEVEN L. NOCK, THE COSTS OF PRIVACY: SURVEILLANCE AND REPUTATION IN AMERICA 73 (1993) (noting that "in a society of strangers . . . so much depends on the faith we have in one another's truthfulness," and that "[l]acking the personal information necessary to discern the veracity of others' claims, we trust instead the monitoring provided by large social structures" and institutions such as credit bureaus).

[149] SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 1-10.

ductive and disconnected from the original context in which it was gathered. This leads to distortion. As H. Jeff Smith observes:

> [D]ecisions that were formerly based on judgment and human factors are instead often decided according to prescribed formulas. In today's world, this response is often characterized by reliance on a rigid, unyielding process in which computerized information is given great weight. Facts that actually require substantial evaluation could instead be reduced to discrete entries in preassigned categories.[150]

Some courts have recognized aggregation as violating a privacy interest. In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the Supreme Court concluded that the disclosure of FBI "rap sheets" was an invasion of privacy within a privacy exemption of the Freedom of Information Act (FOIA).[151] Pursuant to FOIA, "any person" may request "records" maintained by an executive agency.[152] The rap sheets contained extensive information about individuals compiled from a variety of criminal records.[153] FOIA exempts law enforcement records that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."[154] Although the reporters argued that the rap sheets were not private because all of the information in them had already been disclosed, the Court disagreed, noting that in "an organized society, there are few facts that are not at one time or another divulged to another."[155] Thus, the Court observed, there is a "distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole."[156]

Reporters Committee is one of the rare instances where the law has recognized that aggregation can make a material difference in what is known about an individual. Most courts adhere to the secrecy paradigm, which fails to recognize any privacy interest in information publicly available or already disseminated to others.[157] The Restatement

---

[150] H. JEFF SMITH, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA 121 (1994) (footnote omitted).

[151] 489 U.S. 749, 780 (1989).

[152] 5 U.S.C. § 552(a)(3)(A) (2000).

[153] *Reporters Comm.*, 489 U.S. at 749.

[154] 5 U.S.C. § 552(b)(7)(C).

[155] *Reporters Comm.*, 489 U.S. at 763.

[156] *Id.* at 764.

[157] *See, e.g.*, Cordell v. Detective Publ'ns, 307 F. Supp. 1212, 1218 (E.D. Tenn. 1968) ("The Court is of the opinion that the plaintiff may not complain of public disclosure of private facts when the material facts [of concern] are not private but are matters of public record and are in the public domain.").

of Torts declares that for the tort of publicity given to private life, "[t]here is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public. Thus there is no liability for giving publicity to facts about the plaintiff's life that are matters of public record."[158] Similarly, the Restatement provides that for the tort of intrusion upon seclusion, "there is no liability for the examination of a public record concerning the plaintiff."[159] In contrast, aggregation would violate a privacy interest when the aggregation significantly increases what others know about a person, even if originating from public sources.

Differing from *Reporters Committee*, courts have refused to find privacy interests in compilations of information disclosed in Megan's Laws, which involve the dissemination of personal data about convicted sex-offenders.[160] In *Russell v. Gregoire*, the court rejected a constitutional challenge to Washington's Megan's Law because the information was not private since it was "already fully available to the public."[161] Similarly, in *Paul P. v. Verniero*, the Court declined to follow *Reporters Committee* in concluding that New Jersey's Megan's Law was constitutional.[162] As one court observed: "Both the Third Circuit and this Court have repeatedly stressed that *Reporters Committee* is inapposite on the issue of those privacy interests entitled to protection under the United States Constitution."[163] These cases limited *Reporters Committee* to the FOIA context, but they did not supply a reason why recognizing a privacy interest in aggregated data is necessarily linked only to FOIA and does not apply to other areas of law. Legally, the cases have drawn a line, but conceptually, no justification has been offered for the limitation.

Of course, there are many reasons why Megan's Laws might outweigh privacy interests—namely, as a means to promote safety of children, to keep parents informed of which neighbors to avoid, and to

---

[158] RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1965).

[159] *Id.* § 652B cmt. c.

[160] *See, e.g.*, Cutshall v. Sundquist, 193 F.3d 466, 481 (6th Cir. 1999) (concluding that *Reporters Committee* was not applicable to a Megan's Law challenge). *But see* Doe v. Poritz, 662 A.2d 367, 411 (N.J. 1995) (following *Reporters Committee* and recognizing a privacy interest with respect to a sex offender community-notification statute).

[161] 124 F.3d 1079, 1094 (9th Cir. 1997).

[162] 170 F.3d 396, 400, 405 (3d Cir. 1999), *aff'd on reh'g sub nom.* Paul P. v. Farmer, 227 F.3d 98 (3d Cir. 2000) (stating that the holding of *Reporters Committee* dealt with the implication of a privacy interest protected by an exemption to the Freedom of Information Act, not by the Constitution, as in the case of *Paul P.*).

[163] A.A. v. New Jersey, 176 F. Supp. 2d 274, 305 (D.N.J. 2001), *aff'd* 341 F.3d 206 (3d Cir. 2003).

help parents make sure that the babysitter they hired is not a prior child molester. However, *Russell*[164] and *Paul P.*[165] did not recognize a privacy interest in the aggregated data, and thus no balancing took place between this privacy interest and the safety interest.

2. Identification

Although proposed many times in the United States, a national identification card has been explicitly rejected. When the Social Security System was first developed, "President Roosevelt and members of Congress promised that the Social Security card would be kept confidential and would not be used for identification purposes."[166] The cards even stated that they were "not for identification."[167] In 1973, the influential report, *Records, Computers, and the Rights of Citizens*, concluded:

> We take the position that a standard universal identifier (SUI) should not be established in the United States now or in the foreseeable future. By our definition, the Social Security Number (SSN) cannot fully qualify as an SUI; it only approximates one. However, there is an increasing tendency for the Social Security number to be used as if it were an SUI.[168]

Why were there strong negative reactions to identification systems? What is the problem with identifying people?

"Identification" is connecting information to individuals. According to Roger Clarke, identification is "the association of data with a particular human being."[169] Identification enables us to attempt to verify identity—that the person accessing her records is indeed the owner of the account or the subject of the records. Identification enables us not only to confirm the identity of a person, but also to dis-

---

[164] 124 F.3d at 1094.

[165] 170 F.3d at 405.

[166] Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 HARV. J.L. & TECH. 319, 349-50 (2002) (footnote omitted).

[167] *Id.* at 350.

[168] U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS xxxii (1973).

[169] ROGER CLARKE, SMART CARD TECHNICAL ISSUES STARTER KIT, ch. 3 (April 8, 1998), *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/SCTISK3.html. As Clarke observes: "In the context of information systems, the purpose of identification is more concrete: it is used to link a stream of data with a person." Roger Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, 7 INFO. TECH. & PEOPLE 6, 8 (1994), *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html [hereinafter Clarke, *Information Systems*].

cover the perpetrator of a crime from traces left behind, such as fingerprints and genetic material.[170]

Identification is related to disclosure in that both involve the revelation of true information. Identification involves a particular form of true information (one's identity), which enables databases of information to be linked to people. Identification is similar to aggregation as both involve the combination of different pieces of information, one being the identity of a person. However, identification differs from aggregation in that it entails a link to the person in the flesh. For example, there can be extensive aggregations of data about a person in many databases, but these aggregations might be rarely connected to that person as she goes through her day-to-day activities. This is a situation involving high aggregation and low identification. On the flip side, one can have high identification and low aggregation, such as in a world of checkpoints, where people constantly have to show identification but where there are few linkages to larger repositories of data about people.

Identification has many benefits.[171] In order to access various accounts, people's identity must be verified, a step that can reduce fraud and enhance accountability. Identification can deter misleading political campaign ads. Under federal election law, television ads advocating the election or defeat of a candidate must identify the person or group placing the ad.[172] If an ad is not authorized by a candidate, it "shall clearly state the name and permanent street address, telephone number, or World Wide Web address of the person who paid for the communication and state that the communication is not authorized by any candidate or candidate's committee."[173] Identification requirements such as this one can help prevent misinformation and enable people to better assess the ad.

---

[170] For a history of criminal identification techniques, see SIMON A. COLE, SUSPECT IDENTITIES: A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION 4-5 (2001).

[171] *See generally* JOHN D. WOODWARD, JR. ET AL., BIOMETRICS: IDENTITY ASSURANCE IN THE INFORMATION AGE (2003) (commenting that reliable identification improves public safety and the safety of business transactions).

[172] *See* Communications Disclaimer Requirements, 11 C.F.R. § 110.11 (2005) (requiring disclaimers on "general public political advertising"). The identification requirement was originally part of the Federal Election Campaign Act of 1971, Pub. L. No. 92-225, 86 Stat. 3 (1972) (codified as amended at 2 U.S.C. §§ 431-456 (2000 & Supp. II 2002)), which required identification for any expenditure with the purpose of influencing an election. The Court in *Buckley v. Valeo* held that the provision can only apply to speech that "expressly advocate[s] the election or defeat of a clearly identified candidate." 424 U.S. 1, 79-80 (1976).

[173] 2 U.S.C. § 441d(a)(3) (2000 & Supp. II 2002).

Although identification of people or sources of particular messages can be beneficial, it also creates problems. There are some who argue that identification is demeaning to dignity because it reduces people to a number or to bodily characteristics.[174] But, identification is a means to link people to data, not necessarily an indication that people are the equivalent of their identifying characteristics. One need not assume that identification equates individual identity with the identifiers. Therefore, I do not agree that identification is inherently demeaning to dignity.

There is, nonetheless, a more compelling argument for why identification can negatively impact identity. The problem stems not from the identifier itself but from how it links data to individuals. Because it connects people to data, identification attaches informational baggage to people. This alters what others learn about people as they engage in various transactions and activities. An interesting example of this was a case before the European Court of Human Rights (ECHR), which enforces the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms.[175] In *B. v. France*, a French citizen who had surgically changed her sex from male to female sought to have her identification documents (birth certificate, identity card, passport, and voting card) changed from listing her former male name to a female one.[176] Since gender was "indicated on all documents using the identification number issued to everyone" and since this "number was used as part of the system of dealings between social security institutions, employers and those insured," it prevented her from concealing the fact she was a transsexual and effectively assuming a female identity.[177] As the Commission stated:

> A transsexual was consequently unable to hide his or her situation from a potential employer and the employer's administrative staff; the same applied to the many occasions in daily life where it was necessary to prove the existence and amount of one's income (taking a lease, opening a bank account, applying for credit, etc.). This led to difficulties for the social and professional integration of transsexuals.[178]

---

[174] *See* Clarke, *Information Systems*, *supra* note 169, at 32-34 (describing proponents of this view).

[175] Article 8 of the Convention provides for the protection of "the right to respect for [an individual's] private and family life, his home and his correspondence." Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

[176] 232 Eur. Ct. H.R. 33, 36 (1992).

[177] *Id.* at 52.

[178] *Id.*

The Commission concluded that the applicant, "as a result of the frequent necessity of disclosing information concerning her private life to third parties, suffered distress which was too serious to be justified on the ground of respect for the rights of others."[179] This case illustrates how identification can inhibit people's ability to change and can prevent their self-development by tying them to a past from which they want to escape.[180]

In some ways, identification resembles interrogation, as identification often involves the questioning of individuals to compel them to identify themselves. Identification is a component of certain forms of surveillance insofar as it facilitates the detection and monitoring of a person and enables surveillance data to be categorized according to the individuals to which it pertains.

Identification is thus interrelated with other forms of privacy disruption, and, like those forms, it reveals, distorts, and intrudes. Identification diverges, however, because it is primarily a form of connecting data to people. Aggregation creates what I have called a "digital person," a portrait composed of information fragments combined together.[181] Identification goes a step further—it links the digital person directly to a person in realspace.

Some forms of identification can have similar effects to disclosure. For example, expressive methods of identification, such as branding, tattooing, or scarlet letters have been used "usually in the context of slavery, racial subjugation or harsh criminal systems."[182] The identification marker conveys certain information and often bears a particular stigma. In contrast, nonexpressive means of identification, such as fingerprints, identify people without signaling anything to the public.

Identification also creates architectural problems, for it increases the government's power over individuals. Identification has been a critical tool for governments seeking to round up radicals or disfavored citizens.[183] It is also an efficient tool for controlling people. In

---

[179] *Id.*

[180] The science fiction movie *Gattaca* also illustrates these points. Vincent, the protagonist, is linked to his high risk of developing heart problems, thus rendering him unfit for all but the most menial of jobs. GATTACA (Columbia Pictures 1997).

[181] SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 1.

[182] Clarke, *Information Systems*, *supra* note 169, at 20.

[183] As Richard Sobel observes, "[i]dentity systems and documents have a long history of uses and abuses for social control and discrimination." Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37, 48 (2002). Indeed, one of the primary reasons that governments created passports and identity cards was to restrict movement, alter patterns of migration, and control

the United States, passports were used to stifle dissent; since Communists during the McCarthy era were prohibited from using passports, they were restricted from traveling outside the country.[184]

Identification can inhibit one's ability to be anonymous or pseudonymous.[185] Anonymity and pseudonymity protect people from bias based on their identities and enable people to vote, speak, and associate more freely by protecting them from the danger of reprisal.[186] Anonymity can enhance the persuasiveness of one's ideas, for identification can shade reception of ideas with readers' biases and prejudices. This is why, in many universities and schools, exams are graded anonymously. Anonymity provides people with the ability to criticize the companies they work for and to blow the whistle.[187] Anonymity also protects people who read or listen to certain unpopular ideas.[188]

In a series of cases, the Supreme Court has recognized that "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance."[189] Thus, requiring the disclo-

---

the movements of poor people and others viewed as undesirable. Marc Garcelon, *Colonizing the Subject: The Genealogy and Legacy of the Soviet Internal Passport*, *in* DOCUMENTING INDIVIDUAL IDENTITY 83, 86 (Jane Caplan & John Torpey eds., 2001).

[184] Sobel, *supra* note 183, at 49.

[185] Anonymous speech has a long history as an important mode of expression. Between 1789 and 1809, numerous Presidents and Congressmen published anonymous political writings. SMITH, *supra* note 111, at 41. Ben Franklin used over forty pen names during his life. *Id.* at 43. Indeed, James Madison, Alexander Hamilton, and John Jay published the *Federalist Papers* using the pseudonym "Publius." McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 343 n.6 (1995). The Anti-Federalists also used pseudonyms. *Id.*

[186] As Gary Marx notes, anonymity can "facilitate the flow of information and communication on public issues" and "encourage experimentation and risk taking without facing large consequences, risk of failure, or embarrassment since one's identity is protected." Gary T. Marx, *Identity and Anonymity: Some Conceptual Distinctions and Issues for Research*, *in* DOCUMENTING INDIVIDUAL IDENTITY, *supra* note 183, at 311, 316, 318 (2001); *see also* A. Michael Froomkin, *Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 408 (1996) ("Not everyone is so courageous as to wish to be known for everything they say, and some timorous speech deserves encouragement.").

[187] One of the most famous examples of an anonymous whistleblower is Deep Throat, Bob Woodward and Carl Bernstein's confidential source who helped them unearth the Watergate scandal. *See* CARL BERNSTEIN & BOB WOODWARD, ALL THE PRESIDENT'S MEN 71-73, 130-35 (1974).

[188] *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1012-14 (1996) (arguing that reader anonymity is an important First Amendment value and that anonymous reading protects people from being associated with the ideas about which they read).

[189] Talley v. California, 362 U.S. 60, 65 (1960); *see also* Watchtower Bible & Tract Soc. v. Village of Stratton, 536 U.S. 150, 166-67 (2002) (stating that anonymity protects people who engage in "unpopular causes"); *McIntyre*, 514 U.S. at 341-42 ("The decision

sure of identifying information would chill free speech, violating the First Amendment. However, in *Hiibel v. Sixth Judicial District Court*, the Court concluded that a law requiring people to identify themselves during a police stop did not violate the Fourth and Fifth Amendments.[190] In particular, responding to the Fifth Amendment challenge, the Court concluded: "Answering a request to disclose a name is likely to be so insignificant in the scheme of things as to be incriminating only in unusual circumstances."[191] However, as Justice Stevens wrote in dissent:

> A name can provide the key to a broad array of information about the person, particularly in the hands of a police officer with access to a range of law enforcement databases. And that information, in turn, can be tremendously useful in a criminal prosecution. It is therefore quite wrong to suggest that a person's identity provides a link in the chain to incriminating evidence "only in unusual circumstances."[192]

Stevens's dissent recognizes that the harm of identification is often not in the disclosure of the identifying marker (the name, fingerprint, etc.) itself, but in the ability to connect this marker to a stream of collected data. Being asked to identify oneself, therefore, is being asked to link oneself to the data, not just state a name.

3. Insecurity

Identity theft is the fastest growing white collar crime.[193] An identity thief opens accounts and conducts fraud in the victim's name. As I have argued elsewhere, identity theft is made possible because we all have "digital dossiers"—extensive repositories of personal information about us—that are maintained by various companies and institutions.[194] The thief taps into a person's dossier, which becomes polluted with discrediting information when debts go unpaid, or when the thief uses the person's identity to commit a crime. Victims of identity theft are submerged into a bureaucratic hell where, according to one estimate, they must spend approximately two years and almost

---

in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible.").

[190] 542 U.S. 177, 189, 190-91 (2004).

[191] *Id.* at 191.

[192] *Id.* at 196 (Stevens, J., dissenting) (quoting *id.* at 191 (majority opinion)).

[193] Jennifer 8. Lee, *Fighting Back When Someone Steals Your Name*, N.Y. TIMES, Apr. 8, 2001, § 3, at 8.

[194] SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 110.

200 hours to decontaminate their dossier.[195] While their dossier remains defiled, victims have difficulty getting jobs, loans, or mortgages.[196]

Identity theft is the overt result of a larger group of problems I call "insecurity." Glitches, security lapses, abuses, and illicit uses of personal information all fall into this category. Insecurity, in short, is a problem caused by the way our information is handled and protected.

Insecurity is related to aggregation, as it creates risks of downstream harm that can emerge from inadequate protection of compendiums of personal data. Insecurity is also related to identification—it often occurs because of difficulties in linking data to people. As Lynn LoPucki observes, identity theft occurs because "creditors and credit-reporting agencies often lack both the means and the incentives to correctly identify the persons who seek credit from them or on whom they report."[197] In this sense, insecurity can be a cost of lack of identification.[198]

Distortion—the dissemination of false information about a person—is related to insecurity, since problems with security can result in one's records being polluted with false data. This can destroy a person's financial reputation, which today is based in large part on the records maintained by credit reporting agencies.[199] Insecurity, therefore, can involve not only a threat of disclosure, but also a threat of distortion.

Insecurity exposes people to potential future harm. Combating identity theft after it happens has proven immensely difficult.[200] The careless use of data by businesses and the government makes the crime of identity theft incredibly easy. Companies use Social Security numbers (SSNs) as passwords, and since SSNs can be readily obtained

---

[195] JANINE BENNER ET AL., NOWHERE TO TURN: VICTIMS SPEAK OUT ON IDENTITY THEFT, pt. II, §§ 1, 4 (2000), http://www.privacyrights.org/ar/idtheft2000.htm.

[196] SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 110.

[197] Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 94 (2001).

[198] Identification via password, however, can enhance security without linking the individual up to immutable characteristics such as biometric identifiers.

[199] *See* NOCK, *supra* note 148, at 53 (recounting the rise of credit bureaus). For a comprehensive account of the credit reporting system, see EVAN HENDRICKS, CREDIT SCORES & CREDIT REPORTS (2004).

[200] *See* SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 111-12 (noting that investigation and prosecution of identity theft cases is not a top priority for law enforcement agencies, and that victims are slow to realize that their identity has been stolen).

by identity thieves from public records or from database companies, people's accounts and personal information are insecure.[201]

In cases involving the constitutional right to privacy, courts have sometimes recognized insecurity as a privacy harm. In *Whalen v. Roe*, the Supreme Court suggested that the constitutional right to privacy also extended to the "individual interest in avoiding disclosure of personal matters."[202] As the Court observed, the government's collection of personal data for its record systems "is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures."[203] The Court noted that "in some circumstances that duty arguably has its roots in the Constitution."[204] Applying *Whalen*, a federal circuit court in *Fraternal Order of Police, Lodge No. 5 v. City of Philadelphia* concluded that certain questions on a police department employee questionnaire were unconstitutional because there were no guidelines about maintaining the security of the information.[205]

Many privacy statutes require that information be kept secure. This requirement was proposed in the original Fair Information Practices of 1973: "Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data."[206] The Privacy Act of 1974 requires federal agencies maintaining personal data to "establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records."[207] The Children's Online Privacy Protection Act states that websites must protect the "confidentiality, security, and integrity of personal information collected from children."[208] The Gramm-Leach-Bliley Act requires that regulatory agencies of financial institutions establish security standards for personal information.[209] The Health Insurance Portability and Accountability Act of 1996 requires the promulgation of security standards "to ensure the integrity and confidentiality of [medical] information."[210]

---

[201] *Id.* at 115-19.

[202] 429 U.S. 589, 599 (1977).

[203] *Id.* at 605.

[204] *Id.*

[205] 812 F.2d 105, 118 (3d Cir. 1987).

[206] U.S. DEP'T OF HEALTH, EDUC., & WELFARE, *supra* note 168, at 41.

[207] 5 U.S.C. § 552a(e)(10) (2000).

[208] 15 U.S.C. § 6502(b)(1)(D) (2000).

[209] 15 U.S.C. §§ 6801(b), 6805(b)(2) (2000). For the FTC's security regulations, see 16 C.F.R. § 314 (2005).

[210] 42 U.S.C. § 1320d-2(d)(2) (2000).

The Computer Fraud and Abuse Act prohibits hacking into people's computers.[211]

Although the law recognizes injuries when a breach in security results in overt harm to an individual, courts are reluctant to find harm simply from the insecure storage of information.[212] Several privacy statutes attempt to avoid problems in measuring harm by providing for minimum liquidated damages.[213] In many instances, courts ignore insecurity as a problem. For example, in *Board of Education v. Earls*, a school district in Tecumseh, Oklahoma adopted a drug testing policy that required all middle and high school students to undergo drug testing before participating in any extracurricular activity.[214] Some of the students challenged the policy under the Fourth Amendment, but the Supreme Court upheld the testing.[215] The students contended that the school was careless in protecting the security of the test results.[216] Files were not carefully secured and were left where they could be accessed by unauthorized people, such as other students.[217] The Court dismissed this contention because there were no allegations of any improper disclosures.[218] What the court failed to recognize is that disclosure differs from insecurity because the harm caused by disclosure is the actual leakage of information; insecurity is the injury of being placed in a weakened state, of being made more vulnerable to a range of future harms. Although insecurity increases the

---

[211] 18 U.S.C. § 1030 (2000 & Supp. 2002).

[212] *See* Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, *in* SECURING PRIVACY IN THE INTERNET AGE 11-12 (Margaret Jane Radin et al. eds., forthcoming 2006), *available at* http://ssrn.com/abstract=583483 (arguing that the law fails to adequately guard sensitive information, and that a reconceptualization of the legal duties information-keepers owe their customers is necessary).

[213] *See, e.g.*, Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2707(c) (2000) (setting a minimum $1000 fine per violation); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(c) (2000) (setting liquidated damages of $2500 as the minimum amount recoverable from a defendant found to have wrongfully disclosed video tape rental or sale records). The Privacy Act of 1974 also contains a liquidated damages provision; however, the Supreme Court interpreted it to apply only when the plaintiff demonstrates actual damages. *See* Doe v. Chao, 540 U.S. 614, 616 (2004) (construing 5 U.S.C. § 552a(g)(4) (2000)).

[214] 536 U.S. 822, 826 (2002).

[215] *Id.* at 827, 838.

[216] *Id.* at 833.

[217] *Id.* at 848 (Ginsburg, J., dissenting).

[218] *See id.* at 833 (majority opinion) (asserting that because there was no report of a student actually viewing another student's medical record, the carelessness alleged did not rise to the level of a privacy intrusion).

possibility of disclosure, courts will often not recognize a harm unless there has been actual disclosure.

4. Secondary Use

In 1977, in an attempt to capture people engaged in fraud, the federal government began matching its employee records with the records of individuals receiving federal benefits.[219] Some of these government matching programs used information obtained from businesses to uncover fraud.[220] These matchings were done electronically through the use of computers, and they led to the investigations of millions of people.[221] In 1988, Congress passed the Computer Matching and Privacy Protection Act to regulate computer matching.[222]

In 1973, the U.S. Department of Health, Education, and Welfare (HEW) in its influential report on the harms caused by computer databases, set forth a series of Fair Information Practices, one of which provides that "[t]here must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent."[223] This principle, which has become known as the purpose specification principle, has been embodied in various privacy principles and laws. The Privacy Act of 1974, for example, requires agencies to inform people of "the principal purpose or purposes for which the information is intended to be used" when their information is collected.[224] The Fair Credit Reporting Act of 1970 limits the purposes for which credit reports can be used.[225] The Driver's Privacy Protection Act of 1994 makes it "unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted [by the Act]."[226] Anybody who uses an individual's personal

---

[219] REGAN, *supra* note 43, at 86; Robert Gellman, *Does Privacy Law Work?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 193, 198-99 (Philip E. Agre & Marc Rotenberg eds., 1997).

[220] *See* GARY T. MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA 209-10 (1988) (citing instances of government agencies—including the Selective Service and the IRS—using databases supplied by private businesses to investigate instances of draft-dodging and tax fraud).

[221] *Id.* at 208-11.

[222] Computer Matching and Privacy Protection Act (CMPPA) of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (codified at 5 U.S.C. § 552a (2000)).

[223] U.S. DEP'T OF HEALTH, EDUC., & WELFARE, *supra* note 168, at 41-42 (1973).

[224] 5 U.S.C. § 552a(e)(3)(B) (2000).

[225] 15 U.S.C. § 1681b (2000 & Supp. 2002).

[226] 18 U.S.C. § 2722(a) (2000).

data obtained from a motor vehicle record for an impermissible purpose is subject to civil liability.[227] The Cable Communications Policy Act of 1984 requires cable operators to "destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected."[228] The Gramm-Leach-Bliley Act of 1999 places limits on the "reuse" of personal data when a company provides it to another company.[229] The Video Privacy Protection Act of 1988 has a similar provision for personal information collected about video rental customers.[230] The Federal Election Campaign Act states that records of contributors to political committees are "available for public inspection . . . except that any information copied from such reports . . . may not be sold or used by any person for the purpose of soliciting contributions or for commercial purposes."[231] The Health Insurance Portability and Accountability Act regulations restrict secondary uses of medical information beyond those necessary for treatment, payment, and health care operations.[232]

What is the concern over secondary uses of information beyond those purposes for which it is collected? Why are there so many legal attempts to limit secondary uses of data?

"Secondary use" is the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent. There are certainly many desirable instances of secondary use. Information might be used to stop a crime or to save a life. The variety of possible secondary uses of data is virtually infinite, and they range from benign to malignant.

Secondary use can cause problems. It creates a dignitary harm, as it involves using information in ways to which a person does not consent and might not find desirable. Secondary uses thwart people's expectations about how the data they give out will be used. People might not give out data if they know about a potential secondary use, such as for telemarketing, spam, or other forms of intrusive advertising. Fingerprints of United States military recruits originally collected to screen their backgrounds were sent to the FBI and incorporated

---

[227] 18 U.S.C. § 2722 (2000).
[228] 47 U.S.C. § 551(e) (2000).
[229] 15 U.S.C. § 6802(c) (2000).
[230] 18 U.S.C. § 2710(e) (2000).
[231] 2 U.S.C. § 438(a)(4) (2000).
[232] 45 C.F.R. § 164.508(a) (2000).

into the FBI's criminal fingerprint database.[233] Such individuals may not have expected nor desired to have their fingerprints maintained in a law enforcement database of convicts and criminals. Secondary use resembles breach of confidentiality, in that there is a betrayal of the person's expectations when giving out information.

One argument to the contrary is that people should simply expect that their data might be used in different ways when they relinquish it. Under this theory, there is no harm to expectations. But even with privacy policies stating that information might be used in secondary ways, people often do not read or understand these policies. Nor can they appropriately make an informed decision about secondary uses since they might have little idea about the range of potential uses. According to Paul Schwartz, this is an asymmetry of knowledge problem:

> [I]ndividuals are likely to know little or nothing about the circumstances under which their personal data are captured, sold, or processed. This widespread individual ignorance hinders development through the privacy marketplace of appropriate norms about personal data use. The result of this asymmetrical knowledge will be one-sided bargains that benefit data processors.[234]

The potential for secondary use generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability. In this respect, secondary use resembles the harm created by insecurity. The harm is a dignitary one, emerging from denying people control over the future use of their data, which can be used in ways that have significant effects on their lives.

Secondary use also creates architectural problems. The secondary use of information can create problems because the information may not fit as well with the new use. When removed from the original context in which it was collected, data can more readily be misunderstood.

5. Exclusion

Among the Fair Information Practices are three related principles: (1) the existence of record systems cannot be kept secret; (2) an individual must be able to "find out what information about him is in a

---

[233] Pamela Sankar, *DNA-Typing: Galton's Eugenic Dream Realized?*, *in* DOCUMENTING INDIVIDUAL IDENTITY, *supra* note 183, at 273, 278-79.

[234] Schwartz, *supra* note 18, at 1683.

record and how it is used"; and (3) an individual must be able to "correct or amend a record of identifiable information about him."[235] Together these principles aim to allow individuals to have some knowledge of and input into the records about them maintained by government agencies and businesses. The principles require transparency in the record systems and provide individuals with a right to ensure that the information is accurate. What problems or harms are caused when people are not informed about the information entities have about them?

I refer to the failure to provide individuals with notice and input about their records as *exclusion*. There are a number of justifications for exclusion. Providing notice to people about the uses of their personal information and giving them rights to access and correct it can be costly. Also, government agencies might want to keep certain record systems pertaining to law enforcement or intelligence confidential so as not to tip off those who are being investigated.

Exclusion, however, creates an architectural problem. Exclusion reduces accountability on the part of government agencies and businesses that maintain records about individuals. Exclusion is also related to insecurity, as the lack of accountability often goes hand-in-hand with inadequate security in record systems of personal data. Exclusion is different than insecurity in that exclusion is not primarily a harm caused by the lack of protection against data leakage or contamination. Rather, it is a harm created by being shut out from participating in the use of one's personal data, by not being informed about how that data is used, and by not being able to do anything to affect how it is used.

One might contend that exclusion is not a harm in and of itself but is merely a factor that leads to downstream harms like information dissemination. Exclusion, however, can be harmful even if it does not lead to the dissemination of data. As with secondary use and insecurity, exclusion creates a sense of vulnerability and uncertainty in individuals. An inability to participate in the maintenance and use of one's information can lead to feelings of powerlessness and frustration. Some might argue that there are many aspects of life in which we are powerless, and that there is nothing special about powerlessness with respect to personal information. But in a world where personal information is increasingly used to make important decisions

---

[235] U.S. DEP'T OF HEALTH, EDUC., & WELFARE, *supra* note 168, at 41.

about our lives, powerlessness in this arena can be significantly troublesome.

Tort law, by and large, has not recognized exclusion as a harm. In certain kinds of special relationships, however, tort law has developed strong duties and responsibilities. The law of fiduciary duties creates special duties of accountability within certain relationships. A fiduciary relationship exists when one party stands in a special position of power over another person.[236] New York Chief Justice Benjamin Cardozo described the relationship best when he wrote:

> Many forms of conduct permissible in a workaday world for those acting at arm's length, are forbidden to those bound by fiduciary ties. A trustee is held to something stricter than the morals of the market place. Not honesty alone, but the punctilio of an honor the most sensitive, is then the standard of behavior.[237]

Fiduciary relationships have been held to protect privacy in certain relationships.[238] In this way, exclusion is related to the harm of breach of confidentiality, which is discussed later in this taxonomy.[239] Moreover, in certain relationships, such as between doctors and patients, fiduciary duties require informed consent. As one court has noted, "in soliciting the patient's consent, a physician has a fiduciary duty to disclose all information material to the patient's decision."[240] Therefore, tort law has at least recognized the concept of accountability, although courts have not recognized the maintenance of personal information about a person as giving rise to fiduciary obligations. Such a development is not foreclosed, however, as courts "have care-

---

[236] *See* Mobil Oil Corp. v. Rubenfeld, 339 N.Y.S.2d 623, 632 (Civ. Ct. 1972) (defining a fiduciary relationship as one "founded on trust or confidence").

[237] Meinhard v. Salmon, 164 N.E. 545, 546 (N.Y. 1928).

[238] For example, the tort of breach of confidentiality protects the privacy of people's communications with their doctors, bankers, lawyers, and others. *See* Ind. Nat'l Bank v. Chapman, 482 N.E.2d 474, 482 (Ind. Ct. App. 1985) (holding that a bank has a duty not to disclose customer information unless it is to someone with a legitimate public interest); Kohn v. Schiappa, 656 A.2d 1322, 1323 (N.J. Super. Ct. Law Div. 1995) (allowing a claim of negligence where an attorney harmed a client by disclosing confidential information); Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 523 (Ohio 1999) (recognizing a cause of action when physicians breach confidentiality); McCormick v. England, 494 S.E.2d 431, 435 (S.C. Ct. App. 1997) (same). Jessica Litman proposes that the breach of confidentiality tort apply to companies that trade in personal information. Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1304-13 (2000).

[239] *See infra* Part C.1.

[240] Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 483 (Cal. 1990) (en banc).

fully refrained from defining instances of fiduciary relations in such a manner that other and perhaps new cases might be excluded."[241]

The primary legal protection against exclusion is statutory. Federal privacy statutes guard against exclusion by mandating transparency and granting individuals the right to access their information. For example, the Privacy Act provides people the right to access their records.[242] So do the Cable Communications Policy Act,[243] the Fair Credit Reporting Act,[244] and the Children's Online Privacy Protection Act.[245] Several privacy statutes allow people a mechanism to demand the correction of inaccurate information in their records.[246] While these statutes stop short of requiring informed consent, they do give people some ability to discover the information gathered about them.

Some statutes also allow people to opt out of certain uses of information. The Gramm-Leach-Bliley Act, for example, allows people to refuse to allow financial institutions to share their data with third parties.[247] The opt-out right, which assumes consent unless an individual affirmatively indicates a preference for not sharing the information, does not ensure that consent is informed beyond providing customers with notice that information may be shared. Accordingly, it would most likely fail to constitute informed consent within a fiduciary relationship.

C. *Information Dissemination*

Thus far, I have discussed harms arising out of the collection of information as well as harms arising from the storage and use of data. "Information dissemination" is one of the broadest groupings of privacy harms. These harms consist of the revelation of personal data or the threat of spreading information. This group includes (1) breach of confidentiality, (2) disclosure, (3) exposure, (4) increased accessibility, (5) blackmail, (6) appropriation, and (7) distortion.

---

[241] Swerhun v. Gen. Motors Corp., 812 F. Supp. 1218, 1222 (M.D. Fla. 1993) (quoting Quinn v. Phipps, 113 So. 419, 421 (Fla. 1927)).

[242] 5 U.S.C. § 552a(d) (2000).

[243] 47 U.S.C. § 551(d) (2000).

[244] 15 U.S.C. § 1681g(a) (2000).

[245] *Id.* § 6502(b)(1)(B)(i).

[246] *See, e.g.*, Fair Credit Reporting Act, *id.* § 1681i(a)(5)(A).

[247] *See id.* § 6802(b).

1. Breach of Confidentiality

Mrs. McCormick was involved in a contentious divorce and custody battle with her husband. McCormick's doctor gave a letter to her husband that stated that McCormick was suffering from "major depression and alcoholism, acute and chronic."[248] McCormick sued her doctor. According to the court, a "majority of the jurisdictions faced with the issue have recognized a cause of action against a physician for the unauthorized disclosure of confidential information unless the disclosure is compelled by law or is in the patient's interest or the public interest."[249] Unlike the tort of public disclosure, the tort of breach of confidentiality does not require that the disclosure be "highly offensive."[250] The court reasoned that the public disclosure tort "focuses on the *content*, rather than the *source* of the information. The unauthorized revelation of confidential medical information should be protected without regard to the degree of its offensiveness."[251] The tort of breach of confidentiality applies not only to physicians, but also to bankers and other professionals who maintain relationships of trust.[252] Additionally, some courts have extended liability to third parties who induce the physician to disclose.[253]

Why does the law recognize a separate cause of action for breach of confidentiality? Why not rectify such harms with the tort of public disclosure?

The answer, I posit, is that disclosure and breach of confidentiality cause different kinds of injuries. Both involve the revelation of secrets about a person, but breaches of confidentiality also violate the trust in

---

[248] McCormick v. England, 494 S.E.2d 431, 432 (S.C. Ct. App. 1997).

[249] *Id.* at 435 (citations omitted).

[250] *Id.* at 438.

[251] *Id.*

[252] *See, e.g.*, Peterson v. Idaho First Nat'l Bank, 367 P.2d 284, 290 (Idaho 1961) (recognizing a breach of confidentiality tort for disclosure by a bank). For more information on the breach of confidentiality tort, see generally Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426, 1426 (1982) (identifying "the present contours of the . . . tort" and proposing a general rule for its application). Interestingly, England, which does not recognize the privacy torts, does recognize breach of confidence, which has become the country's central means of protecting privacy. RAYMOND WACKS, PRIVACY AND PRESS FREEDOM 48-58 (1995). Unlike the American version, which applies only in a few narrow contexts (mainly to the patient-physician relationship), the English tort applies much more generally and extends even to spouses and lovers. *Id.* at 51.

[253] *See* Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793 (N.D. Ohio 1965) (holding an insurance company liable for inducing a physician to disclose confidential information).

a specific relationship. In this way, the tort emerges from the concept of a fiduciary relationship, which is "founded on trust or confidence reposed by one person in the integrity and fidelity of another."[254]

The harm from a breach of confidence, then, is not simply that information has been disclosed, but that the victim has been betrayed. When it recognized a cause of action for breach of confidentiality in 1920, the court in *Simonsen v. Swenson* noted that "the physician is bound, . . . upon his own professional honor and the ethics of his high profession, to keep secret [a patient's information]. . . . A wrongful breach of such confidence, and a betrayal of such trust, would give rise to a civil action for the damages naturally flowing from such wrong."[255]

Protection against breach of confidentiality helps promote certain relationships that depend upon trust. The disclosure tort also protects relationships of trust, but disclosure must result in the release of embarrassing secrets or discrediting data before courts will consider it to be harmful.[256] Breach of confidentiality requires only a betrayal of trust, regardless of the nature of the data revealed.

There are certainly instances where we might find the breach of confidentiality desirable. In *Simonsen*, for example, the court concluded that a doctor should not be held liable for disclosing the fact that a patient had syphilis, which at the time was believed to be a highly contagious disease.[257] The court held that protecting public health outweighed any privacy interest the plaintiff might have.[258] Likewise, in *Tarasoff v. Regents of the University of California*, a psychotherapy patient murdered a young woman with whom he was obsessed.[259] The court concluded that the patient's psychotherapist had a duty to the woman because he had knowledge that his patient posed a danger to her:

> [T]he therapist's obligations to his patient require that he not disclose a confidence unless such disclosure is necessary to avert danger to others, and even then that he do so discreetly, and in a fashion that would preserve the privacy of his patient to the fullest extent compatible with the prevention of the threatened danger.[260]

---

[254] Mobil Oil Corp. v. Rubenfeld, 339 N.Y.S.2d 623, 632 (Civ. Ct. 1972).
[255] 177 N.W. 831, 832 (Neb. 1920).
[256] *See infra* notes 289-93 and accompanying text.
[257] 177 N.W. at 831.
[258] *Id.* at 832.
[259] 551 P.2d 334, 339-40 (Cal. 1976) (en banc).
[260] *Id.* at 347.

a specific relationship. In this way, the tort emerges from the concept of a fiduciary relationship, which is "founded on trust or confidence reposed by one person in the integrity and fidelity of another."[254]

The harm from a breach of confidence, then, is not simply that information has been disclosed, but that the victim has been betrayed. When it recognized a cause of action for breach of confidentiality in 1920, the court in *Simonsen v. Swenson* noted that "the physician is bound, . . . upon his own professional honor and the ethics of his high profession, to keep secret [a patient's information]. . . . A wrongful breach of such confidence, and a betrayal of such trust, would give rise to a civil action for the damages naturally flowing from such wrong."[255]

Protection against breach of confidentiality helps promote certain relationships that depend upon trust. The disclosure tort also protects relationships of trust, but disclosure must result in the release of embarrassing secrets or discrediting data before courts will consider it to be harmful.[256] Breach of confidentiality requires only a betrayal of trust, regardless of the nature of the data revealed.

There are certainly instances where we might find the breach of confidentiality desirable. In *Simonsen*, for example, the court concluded that a doctor should not be held liable for disclosing the fact that a patient had syphilis, which at the time was believed to be a highly contagious disease.[257] The court held that protecting public health outweighed any privacy interest the plaintiff might have.[258] Likewise, in *Tarasoff v. Regents of the University of California*, a psychotherapy patient murdered a young woman with whom he was obsessed.[259] The court concluded that the patient's psychotherapist had a duty to the woman because he had knowledge that his patient posed a danger to her:

> [T]he therapist's obligations to his patient require that he not disclose a confidence unless such disclosure is necessary to avert danger to others, and even then that he do so discreetly, and in a fashion that would preserve the privacy of his patient to the fullest extent compatible with the prevention of the threatened danger.[260]

---

[254] Mobil Oil Corp. v. Rubenfeld, 339 N.Y.S.2d 623, 632 (Civ. Ct. 1972).
[255] 177 N.W. 831, 832 (Neb. 1920).
[256] *See infra* notes 289-293 and accompanying text.
[257] 177 N.W. at 831.
[258] *Id.* at 832.
[259] 551 P.2d 334, 339-40 (Cal. 1976) (en banc).
[260] *Id.* at 347.

The law, however, is inconsistent in its recognition of breach of confidentiality as a harm. Fourth Amendment law fails altogether to recognize the breach of confidentiality as a harm. In *United States v. Miller*, federal law enforcement officials issued subpoenas to two banks to produce a customer's financial records.[261] The banks complied with the subpoenas, but the customer was not notified of the disclosure of the records until later in the course of prosecution.[262] The defendant contended that the subpoenas violated his Fourth Amendment rights.[263] The Court concluded, however, that the customer lacked a reasonable expectation of privacy in the financial records maintained by his bank.[264] According to the Court, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."[265] Moreover, the Court contended, "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[266]

A few years later, the Court employed similar reasoning in *Smith v. Maryland*, where it held that people lack a reasonable expectation of privacy in the phone numbers they dial because people "know that they must convey numerical information to the phone company" and, therefore, they cannot "harbor any general expectation that the numbers they dial will remain secret."[267]

Miller and *Smith* are the leading cases in what has become known as the "third party doctrine."[268] This doctrine provides that if information is possessed or known by third parties, then, for purposes of the Fourth Amendment, an individual lacks a reasonable expectation of privacy in the information. In the Information Age, much of what we do is recorded by third parties.[269] The third party doctrine therefore

---

[261] 425 U.S. 435, 437 (1976) (limited by Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3421 (2000)).

[262] *Id.* at 438.

[263] *Id.* at 438-39.

[264] *Id.* at 442.

[265] *Id.* at 443.

[266] *Id.* at 442.

[267] 442 U.S. 735, 743 (1979).

[268] SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 201.

[269] *See id.* at 202-09 (discussing the consequences of applying outdated privacy protection schemes to modern times).

places an extensive amount of personal information outside the protection of the Fourth Amendment.[270]

The third party doctrine is based on the secrecy paradigm: since others know the information, it is no longer completely secret. But the fact that the information is known to third parties would not be relevant to the Court's analysis if the harm were understood to be a breach of confidentiality. When people establish a relationship with banks, Internet service providers, phone companies, and other businesses, they are not disclosing their information to the world. They are giving it to a party with implicit (and often explicit) promises that the information will not be disseminated.[271]

Unlike Fourth Amendment law, tort law recognizes breach of confidentiality as a distinct harm. The breach of confidentiality tort applies to the patient-physician relationship and to other relationships as well. As mentioned previously, some courts have held that the tort applies to banks.[272] In *Peterson v. Idaho First National Bank*, the court observed: "All agree that a bank should protect its business records from the prying eyes of the public, moved by curiosity or malice. No one questions its right to protect its fiduciary relationship with its customers, which, in sound banking practice, as a matter of common knowledge, is done everywhere."[273] Not divulging customers' financial information to others "is an implied term of the contract between a banker and his customer."[274] Moreover, the court reasoned: "Inviolate secrecy is one of the inherent and fundamental precepts of the relationship of the bank and its customers or depositors."[275] Many other courts have agreed.[276]

---

[270] *Id.* at 201-02.

[271] *See, e.g.*, Brex v. Smith, 146 A. 34, 36 (N.J. Ch. 1929) (finding an "implied obligation" on banks to keep customers' bank records confidential until compelled by a court to disclose them).

[272] *See supra* note 252 and accompanying text.

[273] 367 P.2d 284, 290 (Idaho 1961) (quoting United States v. First Nat'l Bank of Mobile, 67 F. Supp. 616, 624 (S.D. Ala. 1946)).

[274] *Id.* at 290 (quoting 7 AM. JUR. *Banks* § 196 (1937)).

[275] *Id.*

[276] *See, e.g.*, Barnett Bank of W. Fla. v. Hooper, 498 So. 2d 923, 926 (Fla. 1986) (recognizing that banks establish fiduciary relationships with customers when they enter into transactions); Ind. Nat'l Bank v. Chapman, 482 N.E.2d 474, 482 (Ind. Ct. App. 1985) (finding an implied contract not to disclose personal financial information between a bank and its customers); Suburban Trust Co. v. Waller, 408 A.2d 758, 762 (Md. Ct. Spec. App. 1979) ("[A] bank implicitly warrants to maintain, in strict confidence, information regarding its depositor's affairs."); Richfield Bank & Trust Co. v. Sjogren, 244 N.W.2d 648, 651 (Minn. 1976) (recognizing a duty of confidentiality for banks);

2. Disclosure

The law has developed a number of protections against disclosures of true information about people. The tort of public disclosure of private facts, inspired by Warren and Brandeis's article, creates a cause of action for one who publicly discloses a private matter that is "highly offensive to a reasonable person" and "is not of legitimate concern to the public."[277] In *Whalen v. Roe*, the Supreme Court recognized that the "right to privacy" based on substantive due process also encompassed the "individual interest in avoiding disclosure of personal matters."[278] Although this branch of the right to privacy has not received much further elaboration by the Court, it is recognized in many circuits, where it can enable plaintiffs to sue government officials for disclosing personal information.[279] Further, a number of statutes restrict disclosure of information from government records,[280] school records,[281] cable company records,[282] video records,[283] motor vehicle records,[284] and health records.[285] Various states have restricted

---

McGuire v. Shubert, 722 A.2d 1087, 1091 (Pa. Super. Ct. 1998) (finding a duty for a bank to keep its customers' account information confidential).

[277] RESTATEMENT (SECOND) OF TORTS § 652D (1977); *see* Warren & Brandeis, *supra* note 21, at 195-96.

[278] 429 U.S. 589, 598-99 (1977).

[279] *See, e.g.*, Doe v. Borough of Barrington, 729 F. Supp. 376, 382 (D.N.J. 1990) (holding that it was a violation of the plaintiff's constitutional right to information privacy for police to disclose to neighbors that the plaintiff's husband was infected with AIDS).

[280] *See* Privacy Act of 1974, 5 U.S.C. § 552a(e)(10) (2000) (prohibiting agencies from disclosing information about an individual without her prior written consent).

[281] *See* Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g(b)(1) (2000) (requiring educational agencies or institutions that receive government funding not to disclose education records without written consent).

[282] *See* Cable Communications Policy Act of 1984, 47 U.S.C. §§ 551(b)-(c) (2000) (limiting the extent to which a cable service may collect or disclose personally identifiable information about subscribers).

[283] *See* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b)(1) (2000) (creating civil liability for video stores that disclose personally identifiable information about any customer).

[284] *See* Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (2000) (restricting the use of personal information contained in state motor vehicle records).

[285] *See* Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d-2 (2000) (protecting the privacy of personal health information in transactions).

the disclosure of particular forms of information, such as medical data and alcohol and drug abuse.[286]

Why does the law protect people against the disclosure of true information about them? Some critics of such protections contend that they infringe upon free speech. Eugene Volokh argues that "the right to information privacy—my right to control your communication of personally identifiable information about me—is a right to have the government stop you from speaking about me."[287] Others have charged that protection against disclosure inhibits our ability to judge others and determine whether they are worthy of our trust. According to Richard Posner, disclosure protections provide people the "power to conceal information about themselves that others might use to their disadvantage."[288]

"Disclosure" occurs when certain true information about a person is revealed to others. Disclosure differs from breach of confidentiality because the harm in disclosure involves the damage to reputation caused by the dissemination; the harm with breach of confidentiality is the violation of trust in the relationship.[289] Disclosure can harm even if the information is revealed by a stranger. In *The Right to Privacy*, Warren and Brandeis took issue with the argument that express or implied contractual duties of confidentiality could adequately protect privacy.[290] In particular, they noted that strangers were increasingly able to gather personal information:

> The narrower doctrine [of breach of contract] may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party,

---

[286] *See, e.g.*, CAL. HEALTH & SAFETY CODE § 199.21 (West 1990) (repealed 1995) (prohibiting, inter alia, disclosure of HIV test results); N.Y. PUB. HEALTH LAW § 17 (McKinney 2001) (permitting the release of medical records of minors relating to sexually transmitted diseases and abortion upon written request, but prohibiting the disclosure to parents without consent); 71 PA. STAT. ANN. § 1690.108 (West 1990) (prohibiting the disclosure of all records prepared during alcohol or drug abuse treatment).

[287] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right To Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1050-51 (2000); *see also* THOMAS I. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 556 (1970) ("[T]he right of privacy depends upon guaranteeing an individual freedom from intrusion and freedom to think and believe, not freedom from discussion of his opinions, actions or affairs.").

[288] RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 271 (1983).

[289] *See supra* Part C.1.

[290] Warren & Brandeis, *supra* note 21, at 210.

> the protection granted by the law must be placed upon a broader foundation.[291]

Warren and Brandeis pointed to new technologies of photography. Previously, cameras were large and expensive, and people had to sit and pose for their picture to be taken. This gave rise to a relationship with implicit contractual terms. But the invention of the "snap camera," a smaller camera that could take candid photographs, "rendered it possible to take pictures surreptitiously."[292] This led Warren and Brandeis to conclude that "the doctrines of contract and of trust are inadequate to support the required protection."[293]

Although protecting against disclosure does limit freedom of speech, disclosure can inhibit the very interests free speech protects. Protection from disclosure, like free speech, promotes individual autonomy. The risk of disclosure can prevent people from engaging in activities that further their own self-development.[294] Second, as with free speech, disclosure protections further democratic self-governance. A substantial amount of political discourse does not occur on public soap boxes, but rather in private conversations.[295] Disclosure can inhibit people from associating with others, impinging upon freedom of association, and can also destroy anonymity, which is sometimes critical for the promotion of free expression.[296]

Disclosure can also threaten people's security. For example, many people have good reason to keep their addresses secret, including victims of stalking and domestic abuse attempting to hide from those that threaten them, police officers and prosecutors fearing retaliation by criminals, celebrities desiring to avoid harassment by paparazzi, and doctors who perform abortions desiring to protect their family's safety. People want to protect information that makes them vulnerable or that can be used by others to harm them physically, emotionally, financially, and reputationally. For example, in *Remsburg v. Docusearch, Inc.*, a deranged man was obsessed with Amy Lynn Boyer.[297]

---

[291] *Id.* at 210-11.

[292] *Id.* at 211.

[293] *Id.*

[294] *See* Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 990-92 (2003) [hereinafter Solove, *Virtues*].

[295] *Id.* at 994.

[296] *See id.* at 995 ("Protection against disclosure protects freedom of association, for it enables people to join together and exchange information without having to fear loss of employment, community shunning, and other social reprisals." (footnote omitted)).

[297] 816 A.2d 1001, 1005-06 (N.H. 2003).

He purchased Boyer's Social Security number and employment address from a database company called Docusearch. The man went to Boyer's workplace and murdered her. The court concluded that "threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client."[298]

In many instances, disclosure of information about a person will not enhance our ability to judge her; in fact, it can distort our assessments.[299] Knowing bits and pieces of gossip about a person will often not paint a more complete portrait; it can lead to misimpressions and condemnation without full understanding. Disclosure protections also guard against irrational judgment based on stereotypes of misinformation about diseases.[300] Likewise, society may want to inhibit certain rational judgments, such as employment decisions based on genetic information. Even if employers are correct that a prospective employee with a genetic risk for developing a certain condition is, on balance, riskier to hire than a prospective employee without such a predisposition, even such a rational discriminatory employment decision has its costs. Such decisions may penalize people for things they cannot control and deter people from learning their genetic makeup.[301]

Disclosure can also be harmful because it makes a person a "prisoner of [her] recorded past."[302] People grow and change, and disclosures of information from their past can inhibit their ability to reform their behavior, to have a second chance, or to alter their life's direction. Moreover, when information is released publicly, it can be used in a host of unforeseeable ways, creating problems related to those caused by secondary use.

---

[298] *Id.* at 1008.

[299] *See* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 200 (2000) ("[C]hanges in media technology have increased the risk of mistaking information for knowledge."); Lawrence Lessig, *Privacy and Attention Span*, 89 GEO. L.J. 2063, 2068-69 (2001) (arguing that access to limited amounts of information only "creates the impression of knowledge"); Solove, *Virtues*, *supra* note 294, at 1037 ("Much misunderstanding occurs because of the disclosure of private information . . . .").

[300] *See* Solove, *Virtues*, *supra* note 294, at 1041-42 (describing the stigma attached to those with certain diseases and illnesses).

[301] *Cf. id.* at 1042-43.

[302] U.S. DEP'T OF HEALTH, EDUC., & WELFARE, *supra* note 168, at 112.

The law often protects against disclosure when the information is kept secret but not when others know about it. As one court observed, appearing in public "necessarily involves doffing the cloak of privacy which the law protects."[303] In *Penwell v. Taft Broadcasting Co.*, the court held that a husband and wife wrongfully arrested in public had no privacy interest against the broadcast of video footage of the arrest because it was filmed in public and was "left open to the public eye."[304] Moreover, if a fact about a person is known to others, many courts conclude that it is no longer private. This was the case in *Sipple v. Chronicle Publishing Co.*, where newspapers "outed" Oliver Sipple, who heroically saved President Ford from an assassination attempt.[305] The court concluded that his sexuality was not private because it was well known in the gay community.[306] In *Duran v. Detroit News, Inc.*, a former Colombian judge was attempting to lay low because of death threats and a bounty placed on her head by a drug lord.[307] When a newspaper disclosed her address, a court found no privacy interest because she had revealed it to a few people.[308] A few courts, however, have come to different conclusions regarding whether there is a privacy interest in information communicated to others. For example, in *Times Mirror Co. v. Superior Court*, the identity of a murder witness was disclosed in a newspaper article.[309] Although the witness had confided in a few friends and family members, she had not "rendered otherwise private information public by cooperating in the criminal investigation and seeking solace from friends and relatives."[310]

---

[303] Cefalu v. Globe Newspaper Co., 391 N.E.2d 935, 939 (Mass. App. Ct. 1979).

[304] 469 N.E.2d 1025, 1028 (Ohio Ct. App. 1984) (quoting Jackson v. Playboy Enters., 574 F. Supp. 10, 13 (S.D. Ohio 1983)).

[305] 201 Cal. Rptr. 665, 666 (Ct. App. 1984).

[306] *Id.* at 669 ("[P]rior to the publication of the newspaper articles in question [Sipple]'s homosexual orientation and participation in gay community activities had been known by hundereds of people in a variety of cities . . . .").

[307] 504 N.W.2d 715, 718 (Mich. Ct. App. 1993).

[308] *Id.* at 720 (finding her identity to be "open to the public eye" because her work in Colombia had been disclosed in newspaper articles, and because she had occasionally used her real name in the United States); *see also* Fisher v. Ohio Dep't of Rehab. & Corr., 578 N.E.2d 901, 903 (Ohio Ct. Cl. 1988) (holding that the disclosure of a public conversation between a plaintiff and her fellow employees was not a privacy violation).

[309] 244 Cal. Rptr. 556, 558 (Ct. App. 1988).

[310] *Id.* at 561; *see also* Multimedia WMAZ, Inc. v. Kubach, 443 S.E.2d 491, 500 (Ga. Ct. App. 1994) (finding that the plaintiff's disclosure of his infection status to family, friends, and members of an HIV support group did not render the information public); Y.G. v. Jewish Hosp., 795 S.W.2d 488, 500 (Mo. Ct. App. 1990) (holding that disclosure to doctors and other participants of the plaintiff's in vitro fertilization did not render that information public).

Lior Strahilevitz aptly observes that disclosure involves spreading information beyond existing networks of information flow.[311] The harm of disclosure is not so much the elimination of secrecy as it is the spreading of information beyond expected boundaries. People often disclose information to a limited circle of friends, and they expect the information to stay within this group. Some courts, however, focus on secrecy and do not examine people's expectations of information flow.[312]

3. Exposure

In an 1881 case, *DeMay v. Roberts*, a young unmarried man accompanied a doctor into the room where the doctor was assisting a woman in labor.[313] The court held that the young man had no business being in the room: "It would be shocking to our sense of right, justice and propriety to doubt even but that for such an act the law would afford an ample remedy."[314] Why is it "shocking" for a stranger to watch a woman give birth to a baby?

In 2004, in *National Archives & Records Administration v. Favish*, the Supreme Court rejected a request under the Freedom of Information Act (FOIA) for autopsy photos of Vincent Foster, Jr., a deputy counsel to President Clinton who had committed suicide by shooting himself.[315] The Court concluded that the photos fell under the exemption for records that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."[316] The Court contended: "Family members have a personal stake in honoring and mourning their dead and objecting to unwarranted public exploitation that, by intruding upon their own grief, tends to degrade the rites and respect they seek to accord to the deceased person who was once their own."[317]

---

[311] *See* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 974 (2005) (arguing that an individual has a reasonable expectation of privacy where there is a low risk that the information will spread beyond the individual's social network).

[312] *See id.* at 943-45 (describing "hard-line" cases in which plaintiffs' limited disclosures barred their privacy claims).

[313] 9 N.W. 146, 146 (Mich. 1881).

[314] *Id.* at 148-49.

[315] 541 U.S. 157, 175 (2004).

[316] *Id.* at 171 (quoting 5 U.S.C. § 552(b)(7)(C) (2000))(internal quotation marks omitted).

[317] *Id.* at 168. Courts have also allowed tort suits based on the dissemination of autopsy photos. *See* Reid v. Pierce County, 961 P.2d 333, 339-42 (Wash. 1998) (en

Why is it indecent to publish autopsy photographs? What harm does it cause the families? Imagine that a newspaper prints candid photographs of a person naked or of a person defecating. The person would likely be appalled. But why? We all have genitals. We all defecate. There are no big surprises here.

These are all illustrations of a disruption I call "exposure." Exposure involves the exposing to others of certain physical and emotional attributes about a person. These are attributes that people view as deeply primordial, and their exposure often creates embarrassment and humiliation. Grief, suffering, trauma, injury, nudity, sex, urination, and defecation all involve primal aspects of our lives—ones that are physical, instinctual, and necessary.[318] We have been socialized into concealing these activities.[319]

Although exposure is similar to disclosure—both involve the dissemination of true information—they diverge in an important respect. Exposure is related to disclosure in that concealed information is revealed to others, but the information is not revealing of anything we typically use to judge people's character. Unlike disclosure, exposure rarely reveals any significant new information that can be used in the assessment of a person's character or personality.

Exposure creates injury because we have developed social practices to conceal aspects of life that we find animal-like or disgusting. Further, in certain activities, we are vulnerable and weak, such as when we are nude or going to the bathroom. Norms about nudity and bodily functions have changed throughout history.[320] Martha Nussbaum points out that ancient Romans used toilets whereas "courtiers in Elizabethan England urinated and defecated in corners of palaces, until the stench made it necessary to change residences."[321]

---

banc) (holding that relatives of deceased persons maintained a cause of action for invasion of privacy when coroner's office employees disseminated autopsy photos).

[318] *See, e.g.*, Anita L. Allen, *Lying to Protect Privacy*, 44 VILL. L. REV. 161, 177 (1999) ("Sex is an area in which we encounter our desires, prejudices and shame, and cloak these emotions in privacy.").

[319] *See* NORBERT ELIAS, THE CIVILIZING PROCESS 114 (Edmund Jephcott trans., 1994) (1939) ("The social reference of shame and embarrassment recedes more and more from consciousness. Precisely because the social command not to show oneself exposed or performing natural functions now operates with regard to everyone[,] . . . it seems to the adult a command of his own inner self . . . .").

[320] *See* Solove, *Conceptualizing Privacy*, *supra* note 11, at 1135-36 (observing that public bathing was common in the Middle Ages, but that by the sixteenth century concealment of the body had become the norm).

[321] MARTHA C. NUSSBAUM, HIDING FROM HUMANITY: DISGUST, SHAME, AND THE LAW 115-16 (2004).

In various cultures and at different times in history, levels of reticence and modesty concerning the body have differed greatly.[322] Today's norms and practices, however, call for the concealment of many aspects of the body, bodily functions, and strong displays of emotion. We protect against the exposure of these bodily aspects because this protection safeguards human dignity as defined by modern society. Dignity is a part of being civilized; it involves the ability to transcend one's animal nature.[323]

The need for privacy, and therefore the prevention of exposure, is created by the fact that we have social relationships and concomitant norms of dignity and decorum.[324] "The private arises as a necessary space for the production of civilized behavior," William Ian Miller contends.[325] "Private space enables a civilized public space."[326]

When these practices are disrupted by exposure, people can experience a severe and sometimes debilitating humiliation and loss of self-esteem. Exposure thus impedes a person's ability to participate in society. Even though most people would not view a victim of exposure as a lesser person or as being less civilized, victims feel that way. This is in contrast to disclosure, where information often alters the way a person is perceived.

Disclosure is a power that controls through the imposition of social sanctions and condemnation. Exposure works in a different way, by stripping people of their dignity.[327] Exposure interacts with power-

---

[322] *See* Solove, *Conceptualizing Privacy*, *supra* note 11, at 1135-36 (comparing ancient Greece, where public nudity was seen as a sign of strength, to Renaissance Europe, where "among the wealthy . . . people tried to distance themselves from their body and other's bodies").

[323] *See* WILLIAM IAN MILLER, THE ANATOMY OF DISGUST 177 (1997) ("The civilizing process, according to [Norbert] Elias, means the expansion of the private sphere at the expense of the public. The new norms demand private spaces in which one prepares, grooms, and does the things that would disgust others if they were to be witnessed."); CARL D. SCHNEIDER, SHAME, EXPOSURE, AND PRIVACY 49 (W.W. Norton 1992) (1977) ("The open display of bodily functions—defecating, great pain, the process of dying—threatens the dignity of the individual, revealing an individual vulnerable to being reduced to his bodily existence, bound by necessity.").

[324] Certain activities, such as defecation, we view as uncivilized to perform in front of others. As William Ian Miller observes: "Clearly defecation is degrading and contaminating. It is hedged in with rules about appropriateness as to place. And to violate those rules is a cause for disgrace and shame . . . ." MILLER, *supra* note 323, at 147 (footnote omitted).

[325] *Id.* at 178.

[326] *Id.*

[327] One victim of Chicago's invasive strip search policy testified that "the incident caused her emotional distress that manifested itself in reduced socializing, poor work

ful and potent social norms. When people willingly transgress these norms, society has a strong interest in shaming them, and it is socially beneficial for these norms to be internalized and to result in feelings of shame. However, exposure involves people unwillingly placed in transgression of these norms. We do not view the victims as blameworthy, and there is little social value in their suffering. Nevertheless, due to the internalization of these norms, exposure victims experience strong feelings of shame.

Tort law does not recognize a separate cause of action for exposure; the tort of public disclosure covers both disclosure and exposure.[328] Generally, exposure cases have fared better than ones involving disclosure.[329] For example, in *Daily Times Democrat v. Graham*, air jets blew up a woman's dress while she was at a county fair, exposing her underwear.[330] At that very moment, a photographer for the local newspaper took her photograph, and the picture was printed on the front page of the paper.[331] The woman sued under the public disclosure tort.[332] The newspaper contended that the picture was taken in public, and that, accordingly, there was no privacy interest.[333] This reasoning was based on the secrecy paradigm—that once something is disclosed to the public, it is no longer secret. However, the court concluded that the woman still had a right to be protected from "an indecent and vulgar" violation of privacy under the tort of public disclosure.[334]

Failing to distinguish between disclosure and exposure has adversely affected the recognition of exposure harms in some instances. In *McNamara v. Freedom Newspapers, Inc.*, for example, a newspaper published a picture of a high school athlete whose genitalia was accidentally exposed while playing soccer.[335] The student sued under the

---

performance, paranoia, suicidal feelings, depression, and an inability to disrobe in any place other than a closet." Joan W. v. City of Chicago, 771 F.2d 1020, 1021-22 (7th Cir. 1985).

[328] RESTATEMENT (SECOND) OF TORTS, § 652D (1977).

[329] Eugene Volokh explains that this difference may be because the information revealed via exposure is less useful to those to whom the information is given than that revealed via disclosure. Volokh, *supra* note 287, at 1094.

[330] 162 So. 2d 474, 476 (Ala. 1964).

[331] *Id.*

[332] *Id.* at 476-77.

[333] *Id.* at 477.

[334] *Id.* at 478.

[335] 802 S.W.2d 901, 903 (Tex. App. 1991).

tort of public disclosure of private facts.[336] According to the student, "the Newspaper violated the bounds of public decency."[337] The court conceptualized the injury as one of disclosure and concluded that the picture was not private because "[the student] was voluntarily participating in a spectator sport at a public place."[338] The harm in this case, however, is more appropriately classified as one of exposure. Had the court conceptualized the disruption as one of exposure, the fact that it occurred in a public place would have been much less relevant to the analysis.

4. Increased Accessibility

The federal courts, along with many state courts and agencies, are developing systems to place their records online.[339] These records are readily available at local courthouses or government offices. Nevertheless, placing them online has given rise to an extensive debate over privacy. Some argue that the information is already publicly available, and that therefore it should be available on the Internet in the same manner as it is in physical form at the localities. But many administrative bodies charged with examining the issue have hesitated because of the increased accessibility the Internet will bring. The federal Judicial Conference Committee concluded, for example, that "any benefits of public remote electronic access to criminal files were outweighed by the safety and law enforcement risks such access would create."[340]

If the information is already available to the public, then what is the harm in increasing its accessibility? Increased accessibility does not involve a direct disclosure. Secret information is not disclosed. Rather, information that is already available to the public is made easier to access. Unlike disclosure, the harm is not a direct revealing of information to another. Confidentiality is not breached; the cat is already out of the bag. With increased accessibility, a difference in

---

[336] *Id.*

[337] *Id.* at 905.

[338] *Id.*

[339] *See* SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 131-32 (observing that digital filing requirements and the conversion of paper files to digital format will lead to significant online accessibility of court records).

[340] JUDICIAL CONFERENCE COMM. ON COURT ADMIN. AND CASE MGMT., REPORT ON PRIVACY AND PUBLIC ACCESS TO ELECTRONIC CASE FILES (2001), http://www.privacy.uscourts.gov/Policy.htm.

quantity becomes a difference in quality—it enhances the risk of the harms of disclosure.

Increased accessibility to personal information has many benefits. It enhances openness, allowing people to locate information that they are seeking more easily. Ready accessibility of records enables attorneys to track down people's addresses to serve process. It can assist in investigating the background of a person that one is planning to hire as a child caregiver or teacher. As Robert Gellman notes: "Some basic functions and institutions depend on the public availability of records to operate. The U.S. system of land ownership relies on the public availability of records, although that has not always been the case. The public availability of bankruptcy records is also integral to the process."[341]

Increased accessibility, however, creates problems such as the increased possibility of disclosure. Information can readily be exploited for purposes other than those for which it was originally made publicly accessible. For example, companies are gathering data from public records to use for commercial and marketing purposes or to create dossiers on individuals for profiling and other analysis.[342] As Peter Winn notes, increased access to court records will cause harms to participants in the judicial system: "They will lose . . . their interest in privacy—their identities will be subject to potential misuse by thieves, and their children may be exposed to sexual predators."[343]

Under the secrecy paradigm, courts often view privacy as a binary status—information is either completely private or completely public.[344] Accordingly, once information is released into the public domain, it is no longer private. According to the Restatement, for the tort of public disclosure, "[t]here is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public."[345] For the harm of increased accessibility, however, prior publicity is not dispositive. One must focus on the extent to which the information is made more accessible. Most courts, how-

---

[341] Robert Gellman, *Public Records, Public Policy, and Privacy*, HUMAN RTS., Winter 1999, at 7, 9.

[342] SOLOVE, THE DIGITAL PERSON, *supra* note 40, at 131-32; *see also* Gellman, *supra* note 341, at 7 (warning that although "[p]rivacy protections were inherent in the technology of paper," digitization has led to increased accessibility).

[343] Peter A. Winn, *Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information*, 79 WASH. L. REV. 307, 315 (2004).

[344] See *supra* notes 90-91 and accompanying text for an explanation of the secrecy paradigm.

[345] RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1977).

ever, due to their commitment to the secrecy paradigm, struggle with recognizing this harm.[346] In *Walls v. City of Petersburg*, for example, public employees were compelled to answer a questionnaire asking about the criminal histories of their family members, their complete marital history, their children, and their financial status.[347] The court dismissed their claim that their constitutional right to information privacy was violated, reasoning that there was no privacy interest in the information because it was already available in public records.[348]

In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the Supreme Court recognized the problem of increased accessibility.[349] Earlier in this Article, I noted how this case also recognized the problem of aggregation when the Court concluded that the disclosure of FBI "rap sheets" violated a cognizable privacy interest under FOIA.[350] In addition to concluding that there was a difference between scattered pieces of information and a fully assembled dossier, the Court recognized that "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[351] Here, the Court has recognized the harm of increased accessibility.[352]

5. Blackmail

In nineteenth-century England, sodomy was a serious offense. Although no longer a capital offense—as it had been in the seventeenth century—sodomy still carried harsh penalties from ten years to life in

---

[346] *See, e.g.*, Cline v. Rogers, 87 F.3d 176, 179 (6th Cir. 1996) (holding that the constitutional right to information privacy did not apply to the disclosure of police records because "one's criminal history is arguably not a private 'personal matter' at all, since arrest and conviction information are matters of public record"); Doe v. City of New York, 15 F.3d 264, 268-69 (2d Cir. 1994) (finding that "an individual cannot expect to have a constitutionally protected privacy interest in matters of public record" but that plaintiff's HIV status was not a matter of public record); Scheetz v. Morning Call, Inc., 946 F.2d 202, 207 (3d Cir. 1991) (holding that because information about the victim's claims of spousal abuse potentially "would have wound up on the public record," the victim did not have a privacy interest in the claims).

[347] 895 F.2d 188, 190 (4th Cir. 1990).

[348] *Id.* at 193-94.

[349] *See* 489 U.S. 749, 780 (1989) (observing that the "practical obscurity" of a rap sheet is an important element in personal privacy).

[350] *See supra* notes 151-56 and accompanying text.

[351] *Reporters Comm.*, 489 U.S. at 764.

[352] *Id.* at 780.

prison.[353] Blackmailers would threaten wealthy elites with disclosure of their homosexual activities unless the blackmailers were paid handsomely. The law began to recognize that such forms of extortion should be criminalized. When a blackmail case came to court, courts would awkwardly ignore whether there was any truth to the blackmailer's charges.[354] Certainly not all victims of blackmail were innocent, yet courts offered protection even to those accused of transgressing society's strong sexual taboos and criminal laws. Why were such people protected? If the society so vehemently condemned sodomy at the time, why punish the blackmailers rather than those who may have been guilty of sodomy?

One nineteenth-century English judge contended that blackmail was "one of the worst offenses known to the law."[355] As historian Angus McLaren notes:

> The courts had for centuries reassured the [wealthy] that their good names were protected by the laws on libel and slander. The publicity given to the emergence of the blackmailer raised the horrific possibility that the pillaging of the propertied could be carried out by those who threatened not to tell hurtful lies, but obscene truths.[356]

Blackmail has long posed a conundrum for legal scholars.[357] Blackmail involves coercing an individual by threatening to expose her personal secrets if she does not accede to the demands of the blackmailer, which often involve paying hush money.[358] Why should

---

[353] ANGUS MCLAREN, SEXUAL BLACKMAIL 17 (2002) (noting that there were no executions for sodomy in England after 1836).

[354] *See id.* at 21 (explaining that "[v]ictims who appeared to have engaged in same-sex activities put the courts in a potentially awkward situation," as the courts did not want to exonerate those who had engaged in same-sex activities).

[355] *Id.* at 20 (quoting *Central Criminal Court*, TIMES (London), June 20, 1895, at 3).

[356] *Id.* at 28-29.

[357] *See* LEO KATZ, ILL GOTTEN GAINS 140-45 (1996) (discussing various philosophers' interpretations of the connection between blackmail and coercion and the difficulties of formulating a complete theory). The term "blackmail" originated in Tudor times and referred to extortion in general. MCLAREN, *supra* note 353, at 12. "Modern blackmail first emerged when criminals in the eighteenth century recognized that the laws against sodomy provided them with the means by which they could extort money from those whom they could entrap." *Id.* at 3.

[358] *See* 31A AM. JUR. 2D, *Extortion, Blackmail, and Threats* § 20 (2002) (recognizing that, although statutes differ in form, the use of a threat to extract something is at the heart of blackmail). For a discussion of how blackmail laws protected reputations in different periods of American history, see Lawrence M. Friedman, *Name Robbers: Privacy, Blackmail, and Assorted Matters in Legal History*, 30 HOFSTRA L. REV. 1093, 1112-13 (2002) (observing that blackmail went "against the American grain" of allowing second chances and fresh starts).

society restrict contracts not to divulge secrets? Blackmail does not seem to be about preventing disclosure, for as Joseph Izenberg argues, prohibiting a blackmailer compensation for silence will likely make disclosure more probable.[359] If this is the case, then what interest does the crime of blackmail protect?

Scholars have offered a panoply of hypotheses. Richard Posner argues that blackmail is illegal because it neither maximizes wealth nor provides any net social benefit.[360] In contrast, Gary Anderson and Walter Block contend that blackmail, as distinct from extortion, involves a transaction just like any other, in which both parties bargain for the result they desire.[361] Jennifer Brown finds that blackmail undermines the criminal justice system by enabling private contracts that withhold information from the justice system.[362] Richard Epstein proposes that blackmail is socially detrimental because it "breeds fraud and deceit."[363] According to Wendy Gordon, blackmail is illegal because it involves the blackmailer treating the victim as a means (to earn money) rather than an end.[364] Finally, Richard McAdams argues that blackmail inhibits the development of social norms by stifling public norm enforcement and the discussion and critique of norms.[365]

I posit that blackmail is criminalized because of the power relationship it creates. Blackmail allows a person to be dominated and controlled by another. With blackmail, the harm is not in the actual disclosure of the information, but in the control exercised by the one who makes the threat over the data subject. In some cases, blackmail can also involve information more akin to exposure than disclosure. Breach of confidentiality is also related to blackmail, as a confidant can threaten to disclose a secret in return for money. Blackmail dif-

---

[359] Joseph Isenbergh, *Blackmail From A to C*, 141 U. PA. L. REV. 1905, 1914 (1993) (noting that in any given case, individuals who have obtained valuable information are most likely to disclose it in the presence of a law forbidding bargaining for secrecy with data subjects, though in the long run, such laws will deter potential blackmailers from digging for valuable information).

[360] Richard A. Posner, *Blackmail, Privacy, and Freedom of Contract*, 141 U. PA. L. REV. 1817, 1818-20 (1993).

[361] Walter Block & Gary M. Anderson, *Blackmail, Extortion and Exchange*, 44 N.Y.L. SCH. L. REV. 541, 544-47 (2001).

[362] Jennifer Gerarda Brown, *Blackmail as Private Justice*, 141 U. PA. L. REV. 1935, 1971 (1993).

[363] Richard A. Epstein, *Blackmail, Inc.*, 50 U. CHI. L. REV. 553, 565 (1983).

[364] Wendy J. Gordon, *Truth and Consequences: The Force of Blackmail's Central Case*, 141 U. PA. L. REV. 1741, 1761 (1993).

[365] Richard H. McAdams, *Group Norms, Gossip, and Blackmail*, 144 U. PA. L. REV. 2237, 2243-64 (1996).

fers from disclosure, exposure, and breach of confidentiality in that it involves a threat of disclosure rather than an actual disclosure.

A rough analogy may be made to the crimes of battery and assault. Battery involves actual physical harm, whereas assault is putting a person in fear of physical harm.[366] But there are important differences between blackmail and assault. Unlike assault, where the violence threatened is illegal, with blackmail, the threatened disclosure can be perfectly legal. Indeed, the disclosure might be socially beneficial in that it might reveal that the blackmail victim committed a crime or heinous act. But the threat of disclosure is so profoundly disempowering that society still wants to protect against it. Toward the end of Henrik Ibsen's play, *Hedda Gabler*, Judge Brack, who knows a damaging secret about Hedda Gabler, says to her, "My dearest Hedda, believe me I shall not abuse the position." Hedda replies, "In your power, all the same. At the mercy of your will and demands. And so a slave! A slave!"[367] The more people know about us, the more they can exercise control over us. This is why telling one's deepest secrets to another makes one vulnerable. Prohibiting blackmail prevents people from taking advantage of us with our personal information.

The purpose of restricting blackmail is not to limit disclosure but to prevent the use of the threat of disclosure as a tool for exerting power and dominion over others. Our society prohibits slavery, labor below the minimum wage, dangerous workplace conditions, and quid pro quo sexual harassment even if the victim seemingly consents. The rationale for these prohibitions stems in part from the fact that these acts are so coercive that the consent is not voluntary, and so place excessive power over one person in the hands of another. Blackmail similarly demonstrates the profound danger of the threat of disclosure as an instrument of power over another person. Indeed, criminal codes classify blackmail as a form of extortion, which involves the use of fear or threats to force someone to submit to another's will.[368]

The crime of blackmail thus prevents the use of disclosure, exposure, or breach of confidentiality as a means for exercising power over another person. Dissemination of information is a powerful tool, one

---

[366] *See* RESTATEMENT (SECOND) OF TORTS § 13 (1965) (defining battery); *id.* § 21 (defining assault).

[367] HENRIK IBSEN, *Hedda Gabler*, *in* HEDDA GABLER AND OTHER PLAYS 362 (Una Ellis-Fermor trans., Penguin Books 1961).

[368] *See, e.g.*, CAL. PENAL CODE § 518 (West 1999) (defining extortion as "the obtaining of property from another, with his consent, or the obtaining of an official act of a public officer, induced by a wrongful use of force or fear").

that can be wielded to achieve levels of domination and control that may not be socially beneficial. This is why the threats are usually treated as part of the wrongful act itself.

6. Appropriation

In 1902, in *Roberson v. Rochester Folding Box Co.*, a flour company included a lithograph of Abigail Roberson, a minor, on 25,000 advertisement flyers without her consent.[369] The flyers were captioned, "Flour of the Family."[370] Roberson alleged that she "ha[d] been greatly humiliated by the scoffs and jeers of persons who ha[d] recognized her face and picture on this advertisement, and her good name ha[d] been attacked, causing her great distress and suffering, both in body and mind."[371] The portrait, however, was neither racy nor libelous. "The likeness is said to be a very good one," the court noted, and Roberson was "caused to suffer mental distress where others would have appreciated the compliment to their beauty implied in the selection of the picture for such purposes."[372] The court refused to recognize a remedy based on Warren and Brandeis's article, concluding that such an action was the proper domain of the legislature.[373]

Roberson caused quite a stir. An editorial in *The New York Times* lambasted the decision and noted that it "excited as much amazement among lawyers and jurists as among the promiscuous lay public."[374] Shortly after the decision, a comment in the *Yale Law Journal* criticized the *Roberson* decision for not recognizing a remedy for the "undoubted injury to the plaintiff."[375] The strong criticism of the decision even led one of the judges of the majority to defend the opinion in the *Columbia Law Review*.[376] A year later, New York passed a law creating a cause of action to redress the type of injury Roberson suffered.[377] The law still remains viable today.[378]

---

[369] 64 N.E. 442, 442 (N.Y. 1902).

[370] *Id.*

[371] *Id.* Roberson became so ill that she had to see a physician. *Id.*

[372] *Id.* at 442-43.

[373] *Id.* at 447-48 (applying Warren & Brandeis, *supra* note 21).

[374] Editorial, *The Right of Privacy*, N.Y. TIMES, Aug. 23, 1902, at 8, *reprinted in* Denis O'Brien, *The Right of Privacy*, 2 COLUM. L. REV. 437, 438 (1902).

[375] Comment, *An Actionable Right to Privacy?:* Roberson v. Rochester Folding Box Co., 12 YALE L.J. 35, 36 (1902).

[376] O'Brien, *supra* note 374, at 437.

[377] *See, e.g.*, Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U. L. REV. 703, 717 (1990) (noting that the statutes "made it both a

The tort of appropriation was thus one of the first privacy torts to be recognized after Warren and Brandeis's article. The tort of appropriation occurs when "[o]ne . . . appropriates to his own use or benefit the name or likeness of another."[379] To be liable for appropriation, "the defendant must have appropriated to his own use or benefit the reputation, prestige, social or commercial standing, public interest or other values of the plaintiff's name or likeness."[380]

Why did *Roberson* create such a response? What spurred such an extensive public discussion and prompt legislative action? What is problematic about using a person's name or photograph in an advertisement? After all, one's name and image are often not secret. The picture of Roberson was flattering and did not ruin her reputation. What was the injury?

"Appropriation" is the use of one's identity or personality for the purposes and goals of another. Appropriation, like the privacy disruptions of disclosure and distortion, involves the way an individual desires to present herself to society.

The tort of appropriation has currently lost its way, as courts and commentators have not been able to adequately explain the injury that is redressed by the tort. Two competing accounts of the injury predominate in cases and commentary.[381] Many commentators describe the harm caused by the use of one's likeness for commercial purposes as an affront to dignity; Edward Bloustein argued that the harm caused to an individual by appropriation is the "demeaning and humiliating . . . commercialization of an aspect of personality."[382]

Another rationale for the tort is as a protection of property rights. Prosser, who was profoundly influential in the creation of the four modern privacy torts, viewed the interest protected by the appropriation tort as "not so much a mental as a proprietary one."[383] According to Jonathan Kahn, the "early association of appropriation claims with such intangible, non-commensurable attributes of the self as dignity

---

tort and a misdemeanor . . . to use another's name, portrait, or picture for commercial purposes without the subject's consent").

[378] N.Y. CIV. RIGHTS LAW §§ 50, 51 (McKinney 1992).

[379] RESTATEMENT (SECOND) OF TORTS § 652C (1977).

[380] *Id.* § 652C cmt. c.

[381] *See generally* Robert C. Post, *Rereading Warren and Brandeis: Privacy, Property, and Appropriation*, 41 CASE W. RES. L. REV. 647 (1991) (contrasting the "property" and "dignity" rationales for the tort of appropriation).

[382] Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 987 (1964).

[383] Prosser, *supra* note 20, at 406.

and the integrity of one's persona seems to have been lost, or at least misplaced, as property-based conceptions of the legal status of identity have come to the fore."[384] Courts have transformed a tort's targeted harm from one of appropriation to one of intellectual property. Most contemporary cases recognize that the tort of appropriation protects a "valuable right of property."[385] Loss of property seems to be more readily recognized by courts today than the more amorphous feelings of embarrassment or loss of dignity.[386]

To the extent that the tort remains a way to protect against the loss of dignity, why should we inhibit social use of identities simply to prevent people from feeling demeaned when their identities are commercialized? After all, we allow people to sell their identities to endorse products. Further, we allow vigorous criticism and satire, which can be quite humiliating and injurious to people's dignity.

I contend that there is another important dimension of the harm of appropriation—an interference with freedom and self-development. The early appropriation cases allude to this aspect of the harm. In 1905, Georgia became the first state to recognize a tort based on Warren and Brandeis's article. In *Pavesich v. New England Life Insurance Co.*, a life insurance advertisement used a photograph of Paolo Pavesich next to a photograph of "an ill-dressed and sickly looking person."[387] Under Pavesich's picture, the advertisement stated in part: "In my healthy and productive period of life I bought insurance in the New England Mutual Life Insurance Co."[388] The ad seemed flattering for Pavesich, for he was the paragon of all the success and good fortune that would come to those who purchased insurance.[389]

---

[384] Jonathan Kahn, *Bringing Dignity Back to Light: Publicity Rights and the Eclipse of the Tort of Appropriation of Identity*, 17 CARDOZO ARTS & ENT. L.J. 213, 223 (1999). A new tort, known as the "right of publicity," has emerged to redress violations of property rights in one's name or likeness. *See, e.g.*, 1 MCCARTHY, *supra* note 3, § 5:63 ("Simplistically put, while the appropriation branch of the right of privacy is invaded by an injury to the psyche, the right of publicity is infringed by an injury to the pocketbook." (footnote omitted)) .

[385] DAVID A. ELDER, THE LAW OF PRIVACY § 6:1, at 375 (1991) (quoting McQueen v. Wilson, 161 S.E.2d 63, 66 (Ga. Ct. App.), *rev'd on other grounds*, 162 S.E.2d 313 (Ga. 1968)).

[386] *See* Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 109, 114 (2003) (arguing that Prosser's characterization of appropriation as vindicating property interests obscured the dignitary interests the tort protected, and noting that "[m]odern courts are prone to subsuming the privacy claim under the label of publicity").

[387] 50 S.E. 68, 68 (Ga. 1905).

[388] *Id.* at 69.

[389] *Id.*

Pavesich, however, was not flattered, and he sued.[390] In contrast to the *Roberson* court, the *Pavesich* court recognized a cause of action, reasoning that "the body of a person cannot be put on exhibition . . . without his consent. The right of one to exhibit himself to the public at all proper times, in all proper places, and in a proper manner is embraced within the right of personal liberty."[391] The use of one's likeness for advertising purposes can bring

> even the individual of ordinary sensibility[] to a realization that his liberty has been taken away from him; and, as long as the advertiser uses him for these purposes, he cannot be otherwise than conscious of the fact that he is for the time being under the control of another, that he is no longer free, and that he is in reality a slave.[392]

The court speaks in terms of loss of liberty, not in terms of loss of monetary value. The injury is that Pavesich has been *used* against his will. Similarly, according to Justice Gray's dissent in *Roberson*, "we may not say that the plaintiff's complaint is fanciful, or that her alleged injury is purely a sentimental one."[393] "[T]he conspicuous display of her likeness in various public places has . . . humiliated her by the notoriety and by the public comments it has provoked."[394] Justice Gray alluded to what I believe to be the crux of the harm: unwanted notoriety. The appropriation of Roberson's image forced her to become a public figure. In addition to bringing her unwillingly into the public sphere, the appropriation defined her public role and public persona.

The interest safeguarded by protections against appropriation is control of the way one presents oneself to society. The products and causes people publicly endorse shape their public image. When people are associated with products, they become known in terms of these products. Many public figures take great care with their endorsements because these endorsements shape their public image.[395] Thus,

---

[390] *Id.*

[391] *Id.* at 70.

[392] *Id.* at 80.

[393] Roberson v. Rochester Folding Box Co., 64 N.E. 442, 449 (N.Y. 1902) (Gray, J., dissenting).

[394] *Id.*

[395] For example, in 1903, Thomas Edison sought to enjoin the Edison Polyform Manufacturing Company from using his picture on bottles of a pain reliever that Edison himself had invented earlier in his career. Edison v. Edison Polyform Mfg. Co., 67 A. 392, 392 (N.J. Ch. 1907). The court granted the injunction. *Id.* at 395. Similarly, Jacqueline Onassis sued a clothing company for the use of a lookalike in an advertisement because "she has never permitted her name or picture to be used in connection with the promotion of commercial products. Her name has been used sparingly only in connection with certain public services, civic, art and educational projects which she

appropriation can be harmful even if it is not humiliating, degrading, or disrespectful. Being unwillingly used to endorse a product resembles, in certain respects, being compelled to speak and to represent certain viewpoints.

Protection against appropriation establishes what society considers appropriate for others to do in shaping a person's identity. The harm, then, is an impingement on the victim's freedom in the authorship of her self-narrative, not merely her loss of profits. Prosser, however, used the term "appropriation," which is a word that pertains to property. Perhaps a better word to describe the harm is "exploitation." I continue to use the word appropriation, however, because it has become so commonly known in relation to this kind of harmful activity.

7. Distortion

Defamation law has existed for centuries. Consisting of the torts of libel and slander, defamation law protects against falsehoods that injure a person's reputation. In order to be liable for defamation, one must make "a false and defamatory statement concerning another."[396] A "defamatory" statement "tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him."[397] False light, a more recent tort inspired by the Warren and Brandeis article,[398] protects against giving "publicity to a matter concerning another that places the other before the public in a false light" that is "highly offensive to a reasonable person."[399] It safeguards "the interest of the individual in not being made to appear before the public in an objectionable false

---

has supported." Onassis v. Christian Dior—New York, Inc., 472 N.Y.S.2d 254, 257 (Sup. Ct. 1984).

[396] RESTATEMENT (SECOND) OF TORTS § 558(a) (1977).

[397] *Id.* § 559.

[398] *See, e.g.*, Gary T. Schwartz, *Explaining and Justifying a Limited Tort of False Light Invasion of Privacy*, 41 CASE W. RES. L. REV. 885, 885 (1991) (noting that the Warren and Brandeis article led to decisions which Prosser later labeled as the false light tort).

[399] RESTATEMENT (SECOND) OF TORTS § 652E. Although there is a significant amount of overlap between the two torts, false light has a more expansive view of the harm caused by distortion. While defamation requires the proof of reputational harm, false light does not, and plaintiffs can be compensated solely for emotional distress. Schwartz, *supra* note 398, at 887.

light or false position, or in other words, otherwise than as he is."[400] False light is categorized as one of Prosser's four "privacy" torts.[401]

In addition to false light and defamation, a number of privacy statutes ensure accuracy in record systems. The Privacy Act, for example, enables a person to access and correct her records maintained by government agencies.[402] Likewise, the Fair Credit Reporting Act provides recourse for a person who wants to correct her credit records,[403] and the Family Educational Rights and Privacy Act enables students to review and ensure the accuracy of their school records.[404] Additionally, longstanding privacy principles, such as the Code of Fair Information Practice[405] and the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines, contain provisions for ensuring the accuracy of records.[406] The European Union Data Protection Directive contains a similar provision.[407]

Why are these harms of inaccuracy understood as privacy injuries? Why does the law protect against these harms? Why should people have a right to be judged accurately?

I refer to these harms as "distortion." Distortion is the manipulation of the way a person is perceived and judged by others, and involves the victim being inaccurately exposed to the public. I include distortion in the taxonomy of privacy because of its significant similarity to other privacy disruptions. Distortion, like disclosure, involves the spreading of information that affects the way society views a person. Both distortion and disclosure can result in embarrassment, humiliation, stigma, and reputational harm. They both involve the ability to control information about oneself and to have some limited dominion over the way one is viewed by society. Distortion differs from disclosure, however, because with distortion, the information revealed is false and misleading.

---

[400] RESTATEMENT (SECOND) OF TORTS § 652E cmt. b.

[401] Prosser, *supra* note 20, at 389.

[402] 5 U.S.C. § 552a(d) (2000).

[403] 15 U.S.C. § 1681i (2000).

[404] 20 U.S.C. § 1232g(a)(2) (2000).

[405] *See* U.S. DEP'T OF HEALTH, EDUC., & WELFARE, *supra* note 168, at xx-xxiii (listing and discussing "safeguard requirements" and recommendations for automated personal data systems).

[406] ORG. FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980). For more background on the OECD Guidelines, see Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 773-81 (1999).

[407] Council Directive 95/46, *supra* note 46, art. 6.

Throughout most of western history, one's reputation and character have been viewed as indispensable to self-identity and the ability to engage in public life. For centuries, the loss of social regard has had deleterious effects on one's wealth, prosperity, and employment.[408] Social regard, acceptance, and honor are extremely valuable, and they have power over us because they are integral to how we relate to others. Robert Post observes that defamation law also exists for

> the protection of an individual's interest in dignity, which is to say his interest in being included within the forms of social respect; and the enforcement of society's interest in its rules of civility, which is to say its interest in defining and maintaining the contours of its own social constitution.[409]

Reputation is not merely an individual creation. Although it is true that people work very hard to build their reputations, one's reputation is the product of the judgment of other people in society. Reputation is a currency through which we interact with each other. Protection against distortion structures our interactions because it protects this currency. Distortion not only affects the aggrieved individual; it also affects the society that judges that individual: it interferes with our relationships to that individual, and it inhibits our ability to assess the character of those that we deal with. We are thus deceived in our relationships with others; these relationships are tainted by false information that prevents us from making sound and fair judgments. Distortion's direct impact is felt by the aggrieved individual, but it has effects for all of society. We want to avoid arbitrary and undeserved disruption of social relations.

The enigmatic and devious Iago's comments in William Shakespeare's *Othello* capture the importance of reputation:

> Good name in man and woman, dear my lord,
> Is the immediate jewel of their souls;
> Who steals my purse steals trash: 'tis something, nothing;
> 'Twas mine, 'tis his, and has been slave to thousands.
> But he that filches from me my good name

---

[408] Arlette Farge, *The Honor and Secrecy of Families*, *in* 3 A HISTORY OF PRIVATE LIFE 571, 585 (Roger Chartier ed., Arthur Goldhammer trans., 1989). Heinrich Böll's novella, *The Lost Honor of Katharina Blum*, is a remarkable account of the harm of distortion. *See* HEINRICH BÖLL, THE LOST HONOR OF KATHARINA BLUM (Leila Vennewitz trans., 1975) (featuring a character whose life is ruined due to the publication of misleading information).

[409] Robert C. Post, *The Social Foundations of Defamation Law: Reputation and the Constitution*, 74 CAL. L. REV. 691, 711 (1986).

> Robs me of that which not enriches him
> And makes me poor indeed.[410]

Using the power of reputation, Iago orchestrates a series of distortions to make Othello believe that his wife, Desdemona, is having an affair with his lieutenant, Cassio. These distortions induce Othello into a murderous rage, during which he suffocates his wife. *Othello* illustrates the profound destructiveness of distortion, which tears apart relationships, dissolves trust, and instigates violence.

D. *Invasion*

The final grouping of privacy harms I label as "invasion." Invasion harms differ from the harms of information collection, networking, and dissemination because they do not always involve information. I discuss two types of invasion: (1) intrusion, and (2) decisional interference.

1. Intrusion

For hundreds of years, the law has strongly guarded the privacy of the home.[411] According to William Blackstone, "the law . . . has so particular and tender a regard to the immunity of a man's house, that it stiles it his castle."[412] The law protects the home from trespass by others as well as from nuisances.[413] As Thomas Cooley observed in his famous treatise on constitutional law in 1868, "it is better oftentimes that crime should go unpunished than that the citizen should be liable to have his premises invaded, his trunks broken open, his private books, papers, and letters exposed to prying curiosity, and to the mis-

---

[410] WILLIAM SHAKESPEARE, THE TRAGEDY OF OTHELLO, THE MOOR OF VENICE act 3, sc. 3, ll. 158-64 (Edward Pechter ed., W.W. Norton & Co. 2004) (1623).

[411] The notion that the home was one's "castle" was articulated as early as 1499. *See* Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892, 1894 (1981) (dating the first mention to a report written in 1499); *see also* Semayne's Case, 77 Eng. Rep. 194, 195 (K.B. 1605) ("[T]he house of every one is to him as his . . . castle and fortress.").

[412] 4 WILLIAM BLACKSTONE, COMMENTARIES *223.

[413] Nuisance involves "an invasion of another's interest in the private use and enjoyment of land." RESTATEMENT (SECOND) OF TORTS § 822 (1977). William Blackstone defined private nuisance as "any thing done to the hurt or annoyance of the lands, tenements, or hereditaments of another." 3 WILLIAM BLACKSTONE, COMMENTARIES *216.

constructions of ignorant and suspicious persons."[414] The Fourth Amendment protects the home, as well as one's body and baggage, from searches by government officials.[415] One of the torts inspired by Warren and Brandeis's article is intrusion upon seclusion, which creates a cause of action when one intrudes "upon the solitude or seclusion of another or his private affairs or concerns" if the intrusion is "highly offensive to a reasonable person."[416] Why is it important to protect a safe zone, a private realm free from intrusions?

Understood broadly, these actions are all forms of "intrusion." Intrusion involves invasions or incursions into one's life. It disturbs the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable and uneasy. Protection against intrusion involves protecting the individual from unwanted social invasions, affording people what Warren and Brandeis called "the right to be let alone."[417]

Intrusion is related to disclosure, as disclosure is often made possible by intrusive information gathering activities. Intrusion into one's private sphere can be caused not only by physical incursion and proximity but also by gazes (surveillance) or questioning (interrogation). Intrusion has a certain resemblance to surveillance, in that being stared at for extended periods of time can be quite invasive and penetrating and also disturbing, frightening, and disruptive. Intrusion is also related to interrogation, as people can experience interrogation as a kind of intrusion into their affairs.

The harm caused by intrusion, however, differs from that caused by other types of disruption because intrusion interrupts one's activities through the unwanted presence or activities of another person. The case of *Galella v. Onassis* provides a good illustration of how intrusion is related yet distinct from forms of information gathering.[418] Galella, a paparazzo, routinely harassed Jacqueline Onassis and her children with the late President John F. Kennedy, John and Caroline. To capture pictures, Galella jumped into John's path as he was riding his bike, interrupted Caroline's tennis, and, in the words of the trial

---

[414] THOMAS M. COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH REST UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 306 (1868).

[415] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

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

[417] Warren & Brandeis, *supra* note 21, at 193.

[418] 487 F.2d 986 (2d Cir. 1973).

judge, "insinuated himself into the very fabric of Mrs. Onassis' life."[419] Galella's activities involved monitoring, akin to surveillance, yet they were also physically intrusive.

Intrusion need not involve spatial incursions: spam, junk mail, junk faxes, and telemarketing are disruptive in a similar way, as they sap people's time and attention and interrupt their activities. While many forms of intrusion are motivated by a desire to gather information or result in the revelation of information, intrusion can cause harm even if no information is involved. In particular, intrusion often interferes with solitude, the state of being alone or able to retreat from the presence of others. Indeed, Warren and Brandeis wrote from a tradition of solitude inspired by Ralph Waldo Emerson, Henry David Thoreau, and Emily Dickinson.[420]

For centuries, however, solitude has been criticized as self-indulgent.[421] As Aristotle observed: "Surely it is strange, too, to make the supremely happy man a solitary; for no one would choose the whole world on condition of being alone, since man is a political creature and one whose nature is to live with others."[422] Under this view, solitude is a form of retreat from solidarity, a condition of being isolated and self-interested in which a person can escape her social responsibilities.[423] Too much of such freedom from intrusion can lead to a scattered community, where people distance themselves into isolated enclaves.[424] Why do we want to allow people to have a realm in which they can avoid the presence of others in society?

The protection of a realm of solitude does not merely benefit the individual; it is built into society's structure for a social purpose. Hannah Arendt notes that while the Greeks viewed the public sphere

---

[419] *Id.* at 994 (quoting Galella v. Onassis, 353 F. Supp. 196, 228 (S.D.N.Y. 1972)).

[420] Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 25 (1979).

[421] *See, e.g.*, JANETTE DILLON, SHAKESPEARE AND THE SOLITARY MAN 3-13 (1981) (discussing approaches to solitude before Shakespeare's time, which viewed a solitary life as running counter to the good of the community). Solitude, which became a coveted aspect of existence by the end of the seventeenth century, was viewed by many as dangerous and undesireable during the Middle Ages. *See* Michel Rouche, *Private Life Conquers State and Society*, *in* 1 A HISTORY OF PRIVATE LIFE, *supra* note 408, at 419, 434-35 (describing the concern a ninth-century abbot had for the hermit's solitary life).

[422] ARISTOTLE, ETHICA NICOMACHEA § 1169b, ll. 18-19 (W.D. Ross trans., Clarendon Press 1925) (n.d.).

[423] *See* Michael A. Weinstein, *The Uses of Privacy in the Good Life*, *in* NOMOS, *supra* note 71, at 88, 91-93 (discussing critiques of solitude).

[424] *See* LEWIS MUMFORD, THE CITY IN HISTORY 512-13 (1961) (demonstrating how technological improvements have led to increased isolation).

as having paramount importance, the private sphere was essential to shaping the dimensions and quality of life in the public sphere:

> A life spent entirely in public, in the presence of others, becomes, as we would say, shallow. While it retains its visibility, it loses the quality of rising into sight from some darker ground which must remain hidden if it is not to lose its depth in a very real, non-subjective sense.[425]

In other words, solitude does not detract from a rich public life, but in fact enhances it. Solitude enables people to rest from the pressures of living in public and performing public roles.[426] Too much envelopment in society can be destructive to social relationships. For Thoreau, solitude fosters better social relationships because "we live thick and are in each other's way, and stumble over one another, and I think that we thus lose some respect for one another."[427] Without refuge from others, relationships can become more bitter and tense. Moreover, a space apart from others has enabled people to develop artistic, political, and religious ideas that have had lasting influence and value when later introduced into the public sphere.[428]

Generally, courts recognize intrusion upon seclusion tort actions only when a person is at home or in a secluded place.[429] This ap-

---

[425] HANNAH ARENDT, THE HUMAN CONDITION 71 (1958).

[426] According to philosopher Philip Koch, solitude "gives respite and restoration, a time and a place to lick the wounds of social strife." PHILIP KOCH, SOLITUDE 5 (1994); *see also* WESTIN, *supra* note 19, at 35 ("[N]o individual can play indefinitely, without relief, the variety of roles that life demands. . . . Privacy in this aspect gives individuals, from factory workers to Presidents, a chance to lay their masks aside for rest. To be always 'on' would destroy the human organism.").

[427] HENRY DAVID THOREAU, *Walden*, *in* WALDEN AND OTHER WRITINGS 113 (Barnes & Noble Books 1993) (1854).

[428] Many social, political, and religious leaders began their influential public work with preparations performed in private. *See, e.g.*, JOSEPH BENSMAN & ROBERT LILIENFELD, BETWEEN PUBLIC AND PRIVATE: THE LOST BOUNDARIES OF THE SELF 37 (1979) (describing how a "religious hero['s]" retreat to privacy would inspire followers on his return to the public life); Richard H. Weisberg, *It's a Positivist, It's a Pragmatist, It's a* Codifier*! Reflections on Nietzsche and Stendhal*, 18 CARDOZO L. REV. 85, 92 (1996) (noting that, for Nietzsche, "[t]he great legislator is himself (or herself) conceived of as one whose act of social codification begins with a private program of creative self-fulfillment"). As sixteenth-century French essayist Michel de Montaigne contended, solitude—even for public figures—is not self-indulgent, for "[t]hey have only stepped back to make a better jump, to get a stronger impetus wherewith to plunge deeper into the crowd." MICHEL DE MONTAIGNE, *Of Solitude*, *in* THE COMPLETE ESSAYS OF MONTAIGNE 174, 182 (Donald M. Frame trans., 1958).

[429] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977) ("The defendant is subject to liability . . . only when he has intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs.").

proach is akin to courts recognizing a harm in surveillance only when conducted in private, not in public.[430] However, beyond solitude, people often expect space from others—even when they are with other people. According to sociologist Irwin Altman, we need "personal space," a kind of zone or aura around us to separate ourselves from others.[431] Spatial distance provides for "comfort, ease, and relaxation."[432] Animals maintain "remarkably constant" distances from other animals of the same species.[433] In one series of studies, people placed themselves very close to others, sparking strong reactions of hostility and unease; the intruded-upon subjects quickly reestablished appropriate spatial boundaries.[434] As Robert Post observes, the tort of intrusion upon seclusion upholds rules of civility and social respect.[435] We each have certain "territories of the self," and norms of civility require that we respect others' territories.[436] We can, however, "invite intimacy by waiving our claims to a territory and allowing others to draw close."[437]

Some courts are beginning to recognize realms of exclusion where people can shut others out, even in public.[438] Realms of *exclusion* are not realms of *seclusion*; they are structures for personal space that allow us to interact with others without the interference of the rest of society. Communication and association with others often require freedom from intrusion. For example, when we talk to a friend in a restaurant or another public place, we still need space from other people in order to converse freely. In *Sanders v. American Broadcasting Companies*, an undercover reporter accepted work as a "telepsychic"

---

[430] *See supra* notes 81-104 and accompanying text.

[431] IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, CROWDING 52-54 (Irvington 1981) (1975).

[432] *Id.* at 96.

[433] *Id.* at 52.

[434] *Id.* at 87-89.

[435] Post, *supra* note 44, at 966-68.

[436] *Id.* at 971-73 (citing Erving Goffman, *The Territories of the Self*, *in* RELATIONS IN PUBLIC 28 (1971)).

[437] *Id.* at 973.

[438] *See, e.g.*, Shulman v. Group W Prods., Inc., 955 P.2d 469, 491 (Cal. 1998) (holding that a car accident victim had a privacy interest in her conversation with medical rescuers at the accident scene); Stressman v. Am. Black Hawk Broad. Co., 416 N.W.2d 685, 687-88 (Iowa 1987) (holding that broadcasting video of the plaintiff eating at a restaurant might have violated her privacy interest and noting that "the mere fact a person can be seen by others does not mean that person cannot legally be 'secluded'"(quoting Huskey v. Nat'l Broad. Co., 632 F. Supp. 1282, 1287-88 (N.D. Ill. 1986))).

and surreptitiously videotaped conversations she had at work with her coworkers, including Sanders.[439] Even though Sanders worked in a cubicle where he could readily be seen and overheard by other employees, the court concluded that he had a viable privacy interest: "[T]he concept of 'seclusion' is relative. The mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone."[440]

2. Decisional Interference

In 1965, in *Griswold v. Connecticut*, the Supreme Court held that the Constitution prohibited the government from banning the use of contraceptives by married couples.[441] Although the word "privacy" is not explicitly mentioned anywhere in the Constitution, the Court reasoned that the Constitution provides for a "right to privacy" in the "penumbras" of many of the amendments in the Bill of Rights.[442] The Court noted that "[v]arious guarantees [by the Bill of Rights] create zones of privacy."[443]

In *Eisenstadt v. Baird*, the Court extended the reasoning in *Griswold* to the use of contraceptives by unmarried persons as well.[444] The Court explained that privacy "is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child."[445] Subsequently, the Court held in *Roe v. Wade* that the right to privacy "encompass[es] a woman's decision whether or not to terminate her pregnancy."[446]

Griswold, *Eisenstadt*, and *Baird* all protect against what I call "decisional interference"—that is, governmental interference with people's decisions regarding certain matters of their lives. These cases extend to decisions relating to sex and sexuality, while others extend to decisions concerning the upbringing of one's children.[447] Many commen-

---

[439] 978 P.2d 67, 69-70 (Cal. 1999).

[440] *Id.* at 72 (quoting 1 MCCARTHY, *supra* note 3, § 5.10[A][2]).

[441] 381 U.S. 479, 485-86 (1965).

[442] *Id.* at 484.

[443] *Id.*

[444] 405 U.S. 438 (1972).

[445] *Id.* at 453 (emphasis omitted).

[446] 410 U.S. 113, 153 (1973).

[447] *See, e.g.*, Pierce v. Soc'y of Sisters, 268 U.S. 510, 534-35 (1925) (invalidating an Oregon law requiring parents to send their children to public school, because it "un-

tators have argued that the language of privacy is inappropriate for decisional interference cases, since they primarily concern a harm to autonomy and liberty, not to privacy. Thus, Laurence Tribe argues that the central issue in *Roe v. Wade* is "not privacy, but autonomy."[448] Similarly, Louis Henkin contends that the Supreme Court's substantive due process right-to-privacy cases are about protecting a "zone of autonomy, of presumptive immunity to governmental regulation," not about protecting privacy.[449] What relationship does decisional interference have with the other forms of privacy in the taxonomy?

The decisional interference cases are deeply connected to information privacy.[450] In particular, just a few years after *Roe v. Wade*, the Court explained in *Whalen v. Roe* that the constitutionally protected "zone of privacy" extends not only to the "interest in independence in making certain kinds of important decisions" but also to the "individual interest in avoiding disclosure of personal matters."[451] This gave rise to the constitutional right to information privacy, which, although not developed further by the Supreme Court, has been recognized by most federal circuit courts.[452] *Whalen* involved a challenge to a requirement that physicians report to the state the names and addresses of patients who received prescriptions for certain classes of drugs. The *Whalen* Court linked decisional interference with disclosure by suggesting that "[t]he mere existence in readily available form of the

---

reasonably interfere[d] with the liberty of parents . . . to direct the upbringing and education of children under their control").

[448] LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 1352 (2d ed. 1988).

[449] Louis Henkin, *Privacy and Autonomy*, 74 COLUM. L. REV. 1410, 1410-11 (1974).

[450] Thanks to Neil Richards for pointing this out.

[451] 429 U.S. 589, 599-600 (1977).

[452] *See, e.g.*, *In re* Crawford, 194 F.3d 954, 958 (9th Cir. 1999) ("We agree . . . that the indiscriminate public disclosure of [certain personal information] may implicate the constitutional right to informational privacy."); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990) ("Personal, private information in which an individual has a reasonable expectation of confidentiality is protected by one's constitutional right to privacy."); Kimberlin v. U.S. Dep't of Justice, 788 F.2d 434, 438 (7th Cir. 1986) ("Whether or not Kimberlin has a privacy interest in the information . . . depends upon whether he has a reasonable expectation of privacy in the information."); Barry v. City of New York, 712 F.2d 1554, 1559 (2d Cir. 1983) ("Most courts considering the question . . .appear to agree that privacy of personal matters is a [constitutionally] protected interest . . . ."); J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981) ("Our opinion does not mean . . . there is *no* constitutional right to non-disclosure of private information."); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980) (recognizing that *Whalen* protects "the right not to have an individual's private affairs made public by the government"); Plante v. Gonzalez, 575 F.2d 1119, 1132 (5th Cir. 1978) ("There is another strand to the right to privacy properly called the right to confidentiality.").

information about patients' use of [the] drugs creates a genuine concern that the information will become publicly known and that it will adversely affect their reputations. This concern makes some patients reluctant to use [the drugs] . . . ."[453] By creating a risk of disclosure, the statute inhibited patients' decisions regarding their healthcare.[454] The Court ultimately rejected the plaintiff's challenge because the state provided adequate protection against the "unwarranted disclosure" of the patient information.[455] Thus, *Whalen* illustrates how decisional interference relates to disclosure. *Whalen* also shows how decisional interference bears similarities to increased accessibility, since the existence of information in a government database can increase the potential accessibility of that information.

Decisional interference also resembles insecurity, secondary use, and exclusion, in that all three of these information-processing harms can have a chilling effect on a person's decisions regarding her health and body.

Decisional interference and exposure have been judicially recognized to affect the same aspects of the self—health, the body, sex, and so on. The decisional interference cases track traditional areas that are widely considered to be private, such as the home, family, and body. Decisional interference, therefore, does not apply to all decisions, but only to a subset of decisions; this aspect of decisional interference resembles exposure in its focus on those aspects of life which are socially considered to be the most private.

Decisional interference bears a similarity to the harm of intrusion as both involve invasions into realms where we believe people should be free from the incursions of others. Whereas intrusion involves the unwanted general incursion of another's presence or activities, decisional interference involves unwanted incursion *by the government* into an individual's *decisions* about her personal life. The resemblance is demonstrated by examining the first in the Court's line of right-to-privacy cases, its 1891 decision in *Union Pacific Railway Co. v. Botsford*.[456] There, the Court held that a female plaintiff in a civil action could not be forced to submit to a surgical examination: "To compel any one, and especially a woman, to lay bare the body, or to submit it to the touch of a stranger, without lawful authority, is an indignity, an as-

---

[453] *Whalen*, 429 U.S. at 600.
[454] *Id.*
[455] *Id.* at 600-02.
[456] 141 U.S. 250 (1891).

sault, and a trespass. . . ."[457] The Court emphasized the importance of what Judge Cooley had termed the right "to be let alone" which Warren and Brandeis used in their article one year earlier.[458] While the intrusion at issue in *Botsford* clearly implicated the harms of intrusion and exposure, it also resembled decisional interference. The Court captured this parallel in stating that the right "to be let alone" was "carefully guarded by the common law" and consisted of "the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law."[459]

Another case illustrating the connection between decisional interference and intrusion is *Stanley v. Georgia*, which involved a challenge to an obscenity statute that punished the private possession of obscene material.[460] *Stanley* was cited as support for the constitutional right to privacy in *Roe v. Wade*[461] and *Eisenstadt v. Baird*.[462] Although the material in *Stanley* was obscene and could properly be banned under the First Amendment, the Court concluded that "the Constitution protects the right to receive information and ideas . . . regardless of their social worth."[463] The Court noted that this "right takes on an added dimension" in a "prosecution for mere possession of printed or filmed matter in the privacy of a person's own home."[464] It is a fundamental right "to be free, except in very limited circumstances, from unwanted governmental intrusions into one's privacy."[465] The Court quoted Justice Brandeis's dissent in *Olmstead v. United States*,[466] a Fourth Amendment wiretapping case, in which Brandeis argued that the "makers of our Constitution . . . conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized man."[467]

It is particularly interesting that the Court invoked "the right to be let alone," which was Warren and Brandeis's principle justifying the

---

[457] *Id.* at 252.

[458] *Id.* at 251; Warren & Brandeis, *supra* note 21, at 195.

[459] *Union Pacific*, 141 U.S. at 251.

[460] 394 U.S. 557 (1969).

[461] 410 U.S. 113, 152 (1973).

[462] 405 U.S. 438, 453 (1972).

[463] *Stanley*, 394 U.S. at 564.

[464] *Id.*

[465] *Id.*

[466] 277 U.S. 438 (1928).

[467] *Stanley*, 395 U.S. at 564 (quoting *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting) (internal quotation marks omitted)).

privacy torts.[468] The criminalization of the private possession of obscene material, the Court's reasoning suggests, necessitates governmental intrusion into one's home. The Court noted that people have "the right to be free from state inquiry into the contents of [their] library."[469] Linking decisional interference with intrusion, it stressed that "a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch."[470] Further capturing the relationship between the two categories, Robert Post contends that the intrusion tort protects "territories of the self," which are critical to remaining "an independent and autonomous person."[471]

In *Lawrence v. Texas*, the Court further demonstrated the frequent overlap between decisional interference and intrusion in striking down a law that prohibited consensual homosexual sodomy.[472] The Court reasoned that "adults may choose to enter upon this relationship in the confines of their homes and their own private lives and still retain their dignity as free persons."[473] The statute was unconstitutional because of "its [unjustified] intrusion into the personal and private life of the individual."[474] Moreover, the Court stated:

> Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. In our tradition the State is not omnipresent in the home. And there are other spheres of our lives and existence, outside the home, where the State should not be a dominant presence. Freedom extends beyond spatial bounds.[475]

The Court thus linked decisional interference to intrusion.

Decisional interference also bears an indirect resemblance to blackmail, in that laws restricting consensual private sexual behavior often give rise to blackmail. The *Lawrence* Court noted that in 1955, when crafting the Model Penal Code, the American Law Institute recommended against criminalizing "consensual sexual relations conducted in private"[476] in part because "the statutes regulated private conduct not harmful to others," and because "the laws were arbitrarily

---

[468] *See* Warren & Brandeis, *supra* note 21, at 195.
[469] *Stanley*, 395 U.S. at 565.
[470] *Id.*
[471] Post, *supra* note 44, at 973.
[472] 539 U.S. 558, 578 (2003).
[473] *Id.* at 567.
[474] *Id.* at 578.
[475] *Id.* at 562.
[476] *Id.* at 572 (quoting MODEL PENAL CODE § 213.2 cmt. 2 (1980))

enforced and thus invited the danger of blackmail."[477] Indeed, as Angus McLaren recounts, blackmail historically occurred in the shadow of laws that punished consensual sexual activities in private.[478] McLaren writes: "Society preferred to blame the eruption of blackmail on certain 'dangerous' women and men rather than come to terms with the tension between the laws and the sexual practices that often provided temptation to unscrupulous individuals."[479]

CONCLUSION

In 1960, William Prosser identified just four interests under the rubric of privacy, and focused exclusively on tort law. His effort is far too narrow and far too out-of-date to serve as an effective guide to the privacy problems we face today. In this Article, I have attempted to provide a clearer and more robust account of privacy—one that provides us with a framework for understanding privacy problems. The taxonomy demonstrates that privacy disruptions are different from one another and yet share important similarities. The taxonomy enables us to see privacy in a more multidimensional way.[480]

Although all of the privacy harms I identify in the taxonomy are related in some way, they are not all related in the same way—there is no common denominator that links them all. Privacy violations are a group of related harms, each of which has received at least some recognition in the law. But our understanding of privacy remains in a fog, and the law remains fragmented and inconsistent.

Too many courts and policymakers struggle with even identifying the presence of a privacy problem. Protecting privacy requires careful balancing, as neither privacy nor its countervailing interests are absolute values. Unfortunately, due to conceptual confusion, courts and legislatures often fail to recognize privacy problems, and thus no bal-

---

[477] *Id.* (citing MODEL PENAL CODE § 207.5 cmt. at 277-78 (Tentative Draft No. 4, 1955)). For an interesting discussion of *Lawrence* and public versus private places, see Lior Jacob Strahilevitz, *Consent, Aesthetics, and the Boundaries of Sexual Privacy After* Lawrence v. Texas, 54 DEPAUL L. REV. 671 (2005).

[478] MCLAREN, *supra* note 353, at 6.

[479] *Id.* at 8.

[480] One might ask why we should even retain the term "privacy" if it is simply a broader way to describe a group of different types of harms. Why not simply refer to the particular harms themselves and jettison the term "privacy" altogether? But this view overlooks a key aspect of the way we refer to things and think about them. Although the various harms I identify in the taxonomy are different from one another, and although they do not have a core characteristic in common, they do, as I have shown in this Article, share many important similarities.

ancing ever takes place. This does not mean that privacy should always win in the balance, but it should not be dismissed just because it is ignored or misconstrued.

When translated into the legal system, privacy is a form of protection against certain harmful or problematic activities. The activities that affect privacy are not necessarily socially undesirable or worthy of sanction or prohibition. This fact is what makes addressing privacy issues so complex. In many instances, there is no clear-cut wrongdoer, no indisputable villain whose activities lack social value. Instead, many privacy problems emerge as a result of efficacious activities, much like pollution is an outgrowth of industrial production. With the taxonomy, I have attempted to demonstrate that these activities are not without cost, that they have certain nontrivial effects on people's lives and well-being.

Courts and policymakers often have great difficulty in arriving at a coherent assessment of the various privacy problems and harms that they must address. One common pitfall is viewing "privacy" as a particular kind of harm to the exclusion of all others. As illustrated throughout this Article, courts generally find no privacy interest if information is in the public domain, if people are monitored in public, if information is gathered in a public place, if no intimate or embarrassing details are revealed, or if no new data is collected about a person. If courts and legislatures focused instead on the privacy *problems*, many of these distinctions and determinative factors would matter much less in the analysis. Thus, when analyzing surveillance issues, courts focus on whether the surveillance occurs in public or in private, even though problems and harms can emerge in all settings. Aggregation creates problems even when all of the data is already available in the public domain. The same is true of increased accessibility. For disclosure, the secrecy of the information becomes a central dispositive factor; this approach often misses the crux of the disclosure harm, which is not the revelation of total secrets, but the spreading of information beyond expected boundaries. In intrusion analyses, courts often fail to recognize harm when people are intruded upon in public places, yet the nature of the harm is not limited solely to private places.

At other times, the privacy problem at issue is misconstrued. For example, identification is often understood as a harm created by revealing one's name, but the essence of the problem is being linked to a stream of data, not only a name. Insecurity is often not adequately addressed by the law because a materialized harm has not yet oc-

curred. But insecurity remains a problem, even where there has been no actual disclosure or leakage of embarrassing details. Appropriation is understood primarily as a harm to property interests, and its dignitary dimensions are thus frequently ignored by courts. Further complicating matters is the fact that privacy problems are inconsistently recognized across different areas of the law. For example, tort law readily recognizes and redresses breach of confidentiality, yet Fourth Amendment law ignores it as a harm.

Courts and legislatures respond well to more traditional privacy problems, such as intrusions that are physical in nature, disclosures of deep secrets, or distortion. This is due, in part, to the fact that these problems track traditional conceptions of privacy. In the secrecy paradigm, a privacy violation is understood as the uncovering of a person's hidden world. Physical intrusions are problems that even people in ancient times could experience and understand. But some of the privacy problems we face today are different in nature, and do not track traditional conceptions of privacy. They involve efforts to gain knowledge about an individual without physically intruding or even gathering data directly from them (aggregation), or problems that emerge from the way that the data is handled and maintained (insecurity), the way it is used (secondary use), and the inability of people to participate in its processing (exclusion). Modern privacy problems emerge not just from disclosing deep secrets, but from making obscure information more accessible (increased accessibility) or from consistent observation or eavesdropping (surveillance).

The taxonomy lays down a framework to understand the range of privacy problems, the similarities and differences among them, the relationships among them, and what it is that makes them problematic. By focusing on *activities*, the taxonomy also seeks to emphasize how privacy problems arise. Often, technology is involved in various privacy problems, as it facilitates the gathering, processing, and dissemination of information. Privacy problems, however, are caused not by technology alone, but primarily through *activities* of people, businesses, and the government. The way to address privacy problems is to regulate these activities.

With a framework for identifying and understanding privacy problems, courts and policymakers can better balance privacy considerations against countervailing interests. This Article is thus the beginning of what will hopefully be a more comprehensive and coherent understanding of privacy.