INTRODUCTION

I. CANADIAN PRIVACY LAW ACROSS LEGAL INSTRUMENTS

The right to privacy in Canada is recognized through a combination of constitutional, statutory, and common law principles. Although the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [Charter], examined in Part 3, does not explicitly mention privacy, courts have interpreted s 8 of the Charter, which protects against unreasonable search and seizure, as recognizing a constitutional right to privacy—at least in the context of state action. Canadian privacy law has evolved since then through the recognition of privacy torts, examined in Part 1, and the development of statutory protections, most notably under the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 and provincial privacy legislation, examined in Part 2. These developments address privacy violations in private relationships, particularly in view of the fact that data-driven technologies have transformed how personal information is accessed, shared, and processed. Canadian privacy law has been shaped by broader common law principles and heavily influenced by international developments, particularly from the United States, as the texts in Part 1 and Part 3 show, and the European Union, as the texts in Part 2 show.

II. PRIVACY TORT LAW

Canadian privacy tort law has developed over the years in response to technological changes and shifting societal norms. In particular, Canadian law has seen a growing recognition that privacy violations can cause serious harm, even in the absence of physical injury or financial loss. Privacy torts—civil wrongs that provide legal remedies for invasions of privacy—offer individuals a means of recourse when their private information is wrongfully accessed, used, or disclosed. Courts have recognized that traditional causes of action, such as breach of confidence or defamation, do not always capture the full extent of privacy harms, particularly in the face of mass data collection, social media exposure, and digital surveillance. Consequently, privacy torts have emerged to address gaps in the hope that they provide individuals a means to seek redress for invasions of privacy that may not be covered by constitutional protections against state action and statutory protections focused on commercial activities.

The Court of Appeal for Ontario's decision in *Jones v Tsige*, 2012 ONCA 32 was a pivotal moment in Canadian privacy tort law, as it was the decision that formally recognized intrusion upon seclusion as a stand-alone privacy tort. The Court identified three essential elements for

establishing this tort: First, an unauthorized intrusion into an individual's private affairs or concerns. Second, a reasonable expectation of privacy in the information or activity intruded upon. Third, that the intrusive conduct would be highly offensive or cause distress to a reasonable person. This tort applies primarily to cases of intentional and deliberate privacy invasions, such as unauthorized surveillance, snooping through private communications, or illicit access to personal records. Importantly, *Jones v Tsige* clarified that a plaintiff need not prove actual economic harm or loss, acknowledging that privacy breaches can cause dignitary harm, emotional distress, and loss of autonomy.

III. THE PRIVACY TORT AS IT RELATES TO OTHER TORTS

Another privacy tort recognized in Canada is public disclosure of private facts. This tort applies when an individual's private information is widely disseminated without their consent and where there is no legitimate public interest in the disclosure. To establish liability, a plaintiff must prove three things. First, disclosure of private information to the public. Second, that the information's disclosure would be highly offensive to a reasonable person. Third, that there is no legitimate public interest justifying the disclosure. This tort is important for addressing digital invasions of privacy, where private information—such as medical records, intimate images, or personal correspondence—can be shared instantaneously, at a low cost, and permanently on social media or websites.

Privacy and reputation are closely linked, but they remain distinct interests that people hold. Privacy protects individuals from unwarranted intrusions into their personal lives, while reputation concerns how a person is perceived by others. Although both privacy and reputation harms can result in social, emotional, or economic damage, privacy violations related to disclosures involve exposure of *true* information that an individual has a reasonable expectation of keeping private. On the other hand, defamation addresses statements that harm a person's standing in society so, in Canadian common law, defamation relies on the information being *false*—whereas Quebec civil law sets different qualifications for defamation, which can include true information. The two interests frequently intersect in cases of digital harm—particularly in cases that involve the non-consensual distribution of intimate images, data breaches, or doxxing (malicious public exposure of private information). In these cases, both privacy and reputation injuries can occur simultaneously, and both privacy and defamation actions are often filed simultaneously.

When a plaintiff successfully establishes a privacy violation, they may be entitled to various legal remedies, depending on the nature and severity of the harm. General damages compensate the plaintiff for non-economic losses, including emotional distress, humiliation, and loss of reputation. These harms are particularly significant in privacy cases, where the injury often stems from exposure rather than financial loss. Special damages may be awarded for quantifiable economic harm, such as medical expenses for psychological treatment following a privacy breach or loss of income due to reputational damage. Additionally, courts may issue injunctions to prevent ongoing or future invasions of privacy, such as prohibiting the continued dissemination of unlawfully obtained personal information. In some instances, a declaration of rights may be issued, affirming the plaintiff's privacy interests and setting a legal precedent for future cases.

IV. NEW CHALLENGES

Privacy law routinely faces new challenges because privacy violations are often linked to technological developments and the mass collection, processing, and dissemination of personal data. Privacy tort law must therefore protect against a broad spectrum of digital harms, including cyberstalking and the non-consensual distribution of intimate images. Unauthorized

surveillance, data breaches, data scraping, biometric tracking, and location-based monitoring also fall under privacy law and the privacy torts, even though they protect people from various harms that go beyond their privacy.

Canadian law now needs to adapt to new forms of privacy harm that go beyond traditional notions of intrusion and disclosure. Issues such as surveillance driven by artificial intelligence (AI), deepfakes, and algorithmic decision-making present challenges that require courts to reconsider how privacy torts function in the information economy. Privacy law aims to reflect society's expectations of dignity and autonomy with regards to their personal information, and many protection mechanisms developed with different information interactions in mind are now insufficient.

CHAPTER 1.1

WHAT IS PRIVACY?

Daniel Solove, "Conceptualizing Privacy"

(2002) 90:4 Cal L Rev 1087

2. Limited Access to the Self

A number of theorists conceptualize privacy as "limited access" to the self. This conception recognizes the individual's desire for concealment and for being apart from others. In this way, it is closely related to the right-to-be-let-alone conception, and is perhaps a more sophisticated formulation of that right.

The limited-access conception is not equivalent to solitude. Solitude is a form of seclusion, of withdrawal from other individuals, of being alone. Solitude is a component of limited-access conceptions as well as of the right-to-be-let-alone conception, but these theories extend far more broadly than solitude, embracing freedom from government interference as well as from intrusions by the press and others. Limited-access conceptions recognize that privacy extends beyond merely being apart from others. ...

A number of contemporary theorists also have advanced limited-access conceptions. For philosopher Sissela Bok, privacy is "the condition of being protected from unwanted access by others—either physical access, personal information, or attention." Hyman Gross, a legal theorist of privacy, conceives of privacy as "the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited." According to Ernest Van Den Haag, "Privacy is the exclusive access of a person (or other legal entity) to a realm of his own. The right to privacy entitles one to exclude others from (a) watching, (b) utilizing, (c) invading (intruding upon, or in other ways affecting) his private realm." Legal theorist Anita Allen asserts that "a degree of inaccessibility is an important necessary condition for the apt application of privacy."

David O'Brien argues that there is an important distinction among theorists who propound privacy as limited access formulations. Some view limited access as a choice, a form of individual control over who has access to the self. Others view limited access as a state of existence. Arguing for the latter view, O'Brien claims that privacy "may be understood as fundamentally denoting an existential condition of limited access to an individual's life experiences and engagements." "Privacy is not identical with control over access to oneself, because not all privacy is chosen. Some privacy is accidental, compulsory, or even involuntary."

For O'Brien, privacy boils down to the condition of being alone. This suffers from two problems. First, O'Brien neglects to incorporate into his conception an approach toward understanding the content of the private sphere. Second, O'Brien's conception omits any notion of the individual's power to make certain choices

about revealing aspects of herself to others. For example, O'Brien would claim that a person stranded on a deserted island has complete privacy, but this is better described as a state of isolation. Privacy involves one's relationship to society; in a world without others, claiming that one has privacy does not make much sense. According to sociologist Barrington Moore, "the need for privacy is a socially created need. Without society there would be no need for privacy."

Without a notion of what matters are private, limited-access conceptions do not tell us the substantive matters for which access would implicate privacy. Certainly not all access to the self infringes upon privacy—only access to specific dimensions of the self or to particular matters and information. As a result, the theory provides no understanding of the degree of access necessary to constitute a privacy violation. How much control we should have over access to the self? Proponents of the limited-access conception could respond that privacy is a continuum between absolutely no access to the self and total access. If privacy is such a continuum, then the important question is where the lines should be drawn—that is, what degree of access should we recognize as reasonable? This question can only be answered with an understanding of what matters are private and the value of privacy.

• • •

In *Privacy and the Limits of Law,* legal theorist Ruth Gavison, in an attempt to address these shortcomings, develops the most compelling conception of privacy as limited access. Her aim is to define "a neutral concept of privacy" that is "distinct and coherent" because "the reasons for which we claim privacy in different situations are similar." For Gavison, limited access is the common denominator of privacy: "Our interest in privacy ... is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention." According to Gavison, privacy cannot be understood "as a claim, a psychological state, or an area that should not be invaded ... [or] as a form of control." Unlike many limited access theorists who neglect to elaborate on the value of privacy, Gavison argues that privacy as limited access to the self is valuable in furthering liberty, autonomy, and freedom.

Further, Gavison explains what constitutes limited access, which consists of "three independent and irreducible elements: secrecy, anonymity, and solitude." However, the way that Gavison defines access restricts privacy to matters of withdrawal (solitude) and concealment (secrecy, anonymity). Excluded from this definition are invasions into one's private life by harassment and nuisance and the government's involvement in decisions regarding one's body, health, sexual conduct, and family life. Although Gavison contends that "the collection, storage, and computerization of information" falls within her conception, these activities often do not reveal secrets, destroy anonymity, or thwart solitude. Therefore, although Gavison avoids the broadness and vagueness of most limited-access conceptions, her attempt to define what "access" entails winds up being too narrow.

3. Secrecy

One of the most common understandings of privacy is that it constitutes the secrecy of certain matters. Under this view, privacy is violated by the public disclosure of previously concealed information. According to Judge Richard Posner:

> [T]he word 'privacy' seems to embrace at least two distinct interests. One is the interest in being left alone—the interest that is invaded by the unwanted telephone solicitation, the noisy sound truck, the music in elevators, being jostled in the street, or even an obscene theater billboard or shouted obscenity ... . The other privacy interest,

concealment of information, is invaded whenever private information is obtained against the wishes of the person to whom the information pertains.

The latter privacy interest, "concealment of information," involves secrecy. When talking about privacy as secrecy, Posner defines it as an individual's "right to conceal discreditable facts about himself." Posner sees privacy as a form of self-interested economic behavior, concealing true but harmful facts about oneself for one's own gain. People "want to manipulate the world around them by selective disclosure of facts about themselves." "[W]hen people today decry lack of privacy," Posner argues, "what they want, I think, is mainly something quite different from seclusion; they want more power to conceal information about themselves that others might use to their disadvantage." In a less normatively charged manner, Sidney Jourard emphasizes secrecy with his definition of privacy: "Privacy is an outcome of a person's wish to withhold from others certain knowledge as to his past and present experience and action and his intentions for the future."

The privacy-as-secrecy conception can be understood as a subset of limited access to the self. Secrecy of personal information is a way to limit access to the self. This conception is narrower than limited-access conceptions, as secrecy involves only one aspect of access to the self—the concealment of personal facts. ...

In a variety of legal contexts, the view of privacy as secrecy often leads to the conclusion that once a fact is divulged in public, no matter how limited or narrow the disclosure, it can no longer remain private. Privacy is thus viewed as coextensive with the total secrecy of information. For example, the Court's Fourth Amendment jurisprudence adheres to the notion that matters that are no longer completely secret can no longer be private. As William Stuntz observes, according to the Court, Fourth Amendment privacy "flows out of the interest in keeping secrets, not out of the interest in being free from unreasonable police coercion or from other kinds of dignitary harms that search targets may suffer." In a series of cases, the Court has held there can be no "reasonable expectation of privacy" in things exposed to the public, even if it is highly unlikely that anybody will see or discover them. As the Court observed in *Katz*: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." For example, in *California v Greenwood*, the Court held there is no reasonable expectation of privacy in garbage because it is knowingly exposed to the public: "It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public." Similarly, in *Florida v Riley*, the Court held that the Fourth Amendment did not apply to surveillance of a person's property from an aircraft flying in navigable airspace because the surveillance was conducted from a public vantage point.

A number of theorists have claimed that understanding privacy as secrecy conceptualizes privacy too narrowly. Legal theorist Edward Bloustein as well as anthropologist Arnold Simmel have criticized the theory of privacy as secrecy as failing to recognize group privacy. By equating privacy with secrecy, this formulation fails to recognize that individuals want to keep things private from some people but not others. Criticizing a boss to a coworker does not mean that the employee desires that her boss know her comments. Being a member of an organization, especially an unpopular one, is also regarded by many as a private matter. Further, the conception of privacy as secrecy maintained by many courts views secrecy as tantamount to total secrecy rather than selective secrecy. As sociologist Edward Shils notes, contrary to privacy as secrecy, the individual does not intend an act of disclosure to be limitless. "Meaningful discussion of privacy," legal scholar

Kenneth Karst states, "requires the recognition that ordinarily we deal not with an interest in total nondisclosure but with an interest in selective disclosure."

Some theorists attempt to avoid these problems by focusing on selective secrecy. For example, Amitai Etzioni defines privacy as "the realm in which an actor (either a person or a group, such as a couple) can legitimately act without disclosure and accountability to others." Nevertheless, even under the selective secrecy conception, the harm caused by an invasion of privacy is understood as the disclosure of previously concealed information. Privacy, however, involves more than avoiding disclosure; it also involves the individual's ability to ensure that personal information is used for the purposes she desires. According to philosopher Judith Wagner DeCew, secrecy is certainly not coextensive with privacy; secret information is often not private (for example, secret military plans) and private matters are not always secret (for example, one's debts).

We often expect privacy even when in public. Not all activities we deem as private occur behind the curtain. The books we read, the products we buy, the people we associate with—these are often not viewed as secrets, but we nonetheless view them as private matters. As philosopher Julie Inness observes, privacy as secrecy omits the element of control: "[P]rivacy might not necessarily be opposed to publicity; its function might be to provide the individual with control over certain aspects of her life." This sentiment was also recognized by Stanley Benn, who observed that privacy is not that one's private affairs "are kept out of sight or from the knowledge of others that makes them private. Rather, [one's private affairs] are matters that it would be inappropriate for others to try to find out about, much less report on, without one's consent."

In elaborating upon the privacy exemption of the Freedom of Information Act ("FOIA"), the Supreme Court appeared to understand the imperfections of understanding privacy as secrecy. ... In other words, the Court recognized that the accessibility of information, not the mere secrecy of it, was important to protecting privacy. However, the Court has failed to recognize this insight in other contexts.

Therefore, while most theorists would recognize the disclosure of certain secrets to be a violation of privacy, many commonly recognized privacy invasions do not involve the loss of secrecy. Secrecy as the common denominator of privacy makes the conception of privacy too narrow.

4. Control Over Personal Information

One of the most predominant theories of privacy is that of control over personal information. According to Alan Westin: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Numerous other scholars have articulated similar theories. Arthur Miller declares that "the basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him." According to Charles Fried, "Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves." President Clinton's Information Infrastructure Task Force has defined privacy as "an individual's claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed, and used." The Supreme Court has even stated that privacy is "control over information concerning his or her person."

The control-over-information can be viewed as a subset of the limited access conception. The theory's focus on information, however, makes it too narrow a conception, for it excludes those aspects of privacy that are not informational,

such as the right to make certain fundamental decisions about one's body, reproduction, or rearing of one's children.

Additionally, the theory is too vague because proponents of the theory often fail to define the types of information over which individuals should have control. ...

Some theorists attempt to define the scope of what constitutes personal information over which individuals should exercise control, but their attempts run into significant difficulties. For example, legal scholar Richard Parker's theory defines the scope of personal information extremely broadly: "Privacy is control over when and by whom the various parts of us can be sensed by others." "Control over who can see us, hear us, touch us, smell us, and taste us, in sum, control over who can sense us, is the core of privacy." Parker's definition would make most interpersonal contact in society a privacy invasion because it brings unwanted access to the self. Yet, we are frequently seen and heard by others without perceiving it as even the slightest invasion of privacy.

Charles Fried links his definition of the scope of personal information to the value of privacy. He defines privacy as "control over knowledge about oneself" that is necessary to protect "fundamental relations" of "respect, love, friendship and trust." His theory speaks about the value of privacy (promoting respect, love, friendship, and trust) and presumably, would define the scope of information as "intimate" information (information necessary to form and foster relationships involving respect, love, friendship, and trust). However, looking at only intimate information excludes important information such as financial records.

Finally, one could limit the scope of personal information to that which relates to the individual. Richard Murphy defines the scope of personal information as consisting of "any data about an individual that is identifiable to that individual." Murphy's definition is too broad because there is a significant amount of information identifiable to us that we do not deem as private. For example, the fact that a person is a well-known politician is identifiable to her, but is not private. Murphy's definition thus provides no reasonable limitation in scope.

In addition to failing to adequately define the scope of information, the conceptions of privacy as control over information fail to define what is meant by "control" over information. Theorists provide little elaboration as to what control really entails, and it is often understood too narrowly or too broadly. Frequently, control is understood as a form of ownership in information. For example, Westin concludes that "personal information, thought of as the right of decision over one's private personality, should be defined as a property right." This notion is partially embodied in the tort of commercial appropriation, which protects people against others' using their image or likeness for commercial gain.

The notion that individuals have a property right in information about themselves can be traced to John Locke, who asserted that individuals have property rights in their person and the fruits of their labor. According to Locke, privacy flows naturally from selfhood: "[E]very man has a *property* in his own *person*." From this principle, Locke deduced that property extends to the products of one's labor: "Whatsoever then he removes out of the state that nature hath provided, and left it in, he hath mixed his *labor* with, and joined it to something that is his own, and thereby makes it his *property*." ...

Personal information as property is justified by viewing it as an extension of personality. As the authors of our own lives, we generate information as we develop our personalities. The growth of individualism spawned the "belief that one's actions and their history 'belonged' to the self which generated them and were to be shared only with those with whom one wished to share them." "One's self—for other people—is one's expression of one's self," observes Madame Merle in

Henry James's Portrait of a Lady, "and one's house, one's furniture, one's garments, the books one reads, the company one keeps—these things are all expressive."

Given the unique nature of information, the extension of these concepts to personal information does not come without some difficulties. Information can be easily transmitted, and once known by others, cannot be eradicated from their minds. Unlike physical objects, information can be possessed simultaneously within the minds of millions. This is why intellectual property law protects particular tangible expressions of ideas rather than the underlying ideas themselves. The complexity of personal information is that it is both an expression of the self as well as a set of facts, a historical record of one's behavior.

Further, there are problems with viewing personal information as equivalent to any other commodity. Personal information is often formed in relationships with others, with all parties to that relationship having some claim to that information. For example, individuals are not the lone creators of their web-browsing information, for most of that information is created from the interaction between the user and websites. Often, the market value of information is not created exclusively by the labor of the individual to whom it relates but in part by the third party that compiles the information. For example, the value of personal information for advertisers and marketers emerges in part from their consolidation and categorization of that information.

An example of the difficulty in assigning ownership to information is illustrated by *Haynes v Alfred A. Knopf, Inc*. This case involved Nicholas Lemann's highly praised book about the social and political history of African Americans who migrated from the South to northern cities. The book chronicled the life of Ruby Lee Daniels, who suffered greatly from her former husband Luther Haynes's alcoholism, selfishness, and irresponsible conduct. Haynes sued the author and the publisher under the public disclosure of private facts tort, claiming that he had long since turned his life around and that the disclosure of his past destroyed the new life he had worked so hard to construct. Judge Posner, writing for the panel, concluded that there could be no liability for invasion of privacy because "[a] person does not have a legally protected right to a reputation based on the concealment of the truth" and because the book narrated "a story not only of legitimate but of transcendent public interest."

Although it did not hinge on the shared nature of the information, this case illustrates that personal information rarely belongs to just one individual; it is often formed in relationships with others. Ruby Daniels's story was deeply interwoven with Haynes's story. Daniels had a right to speak about her own past, to have her story told. This was her life story, not just Luther Haynes's. In sum, understanding control as ownership presents difficulties in grappling with the unique shared nature of much private information. A claim of privacy is not the same as a claim of ownership.

Not only does defining control prove difficult, control over information is too broad a conception. Gerety claims that Westin's definition "on its face includes all control over all information about oneself, one's group, one's institutions. Surely privacy should come, in law as in life, to much less than this." According to Inness, not all personal information is private; she contends that "it is the intimacy of this information that identifies a loss of privacy." Thus one possibility is that the control-over-information conception could be limited in scope by including only intimate information.

Even if narrowed to include only intimate information, however, the conception is still too broad. According to DeCew, we often lose control over information in ways that do not involve an invasion of our privacy. To illustrate this point,

Daniel Farber invokes the example of the flasher. A flasher is controlling the visual access to his body by allowing it, yet preventing flashing is not a violation of the flasher's privacy; rather, flashing is seen as a violation of the privacy of others.

David O'Brien also criticizes the conception of privacy as the control of information for being too narrow. Many privacy interests involve an individual's "freedom to engage in private activities" rather than the disclosure or nondisclosure of information. O'Brien correctly recognizes that privacy is invaded not just by intrusions into information but also by nuisances such as noises, smells, and other noxious disruptions of one's peace of mind. As DeCew points out, the conception of privacy as control over information is too narrow because privacy is not reducible to personal information. Privacy, contends DeCew, can be invaded even if nobody else knows something new about a person, such as by being forced to hear propaganda, by being manipulated by subliminal advertisements, or by being disrupted by a nuisance that thwarts one's ability to think or read. In other words, the theory of privacy as control over information excludes many aspects of life that we commonly assume to be private. Anita Allen similarly critiques the control-over-information conception for omitting issues such as abortion and sexual freedom.

Additionally, some theorists critique the control-over-personal-information conception as being too narrow because it focuses too heavily on individual choice. Paul Schwartz argues that the conception of information control wrongly assumes that individuals have the autonomy to exercise control over their personal data in all situations, an assumption that fails to recognize "that individual self-determination is itself shaped by the processing of personal data." Schwartz also questions the assumption that individuals are able to exercise meaningful choices with regard to their information, given disparities in knowledge and power when bargaining over the transfer of their information. The implication is that privacy involves not only individual control, but also the social regulation of information. In other words, privacy is an aspect of social structure, an architecture of information regulation, not just a matter for the exercise of individual control.

To summarize, conceptualizing privacy as control over personal information can be too vague, too broad, or too narrow. Conceptions of information control are too vague when they fail to define what types of information over which individuals should have control. When theorists attempt to define what constitutes "personal information," the conceptions become overly limited or expansive. Further, when theorists attempt to define what "control" entails, they often define it as a form of ownership, making the conception falter in a number of respects. Finally, conceptions of information control are too narrow because they reduce privacy to informational concerns, omit decisional freedom from the realm of privacy, and focus too exclusively on individual choice.

5. Personhood

Another theory of privacy views it as a form of protecting personhood. Building upon Warren and Brandeis's notion of "inviolate personality," Paul Freund coined the term "personhood" to refer to "those attributes of an individual which are irreducible in his selfhood."

The theory of privacy as personhood differs from the theories discussed earlier because it is constructed around a normative end of privacy, namely the protection of the integrity of the personality. This theory is not independent of the other theories, and it often is used in conjunction with the other theories to explain why privacy is important, what aspects of the self should be limited, or what information we should have control over.

a. Individuality, Dignity, and Autonomy

What is personhood? What aspects of the self does privacy protect? According to Edward Bloustein, privacy protects individuality. Privacy is a unified and coherent concept protecting against conduct that is "demeaning to individuality," "an affront to personal dignity," or an "assault on human personality." Jeffrey Reiman also recognizes a personhood component to privacy: "The right to privacy ... protects the individual's interest in becoming, being, and remaining a person."

Philosopher Stanley Benn also develops a personhood conception of privacy, noting that privacy amounts to respect for individuals as choosers: "[R]espect for someone as a person, as a chooser, implie[s] respect for him as one engaged on a kind of self-creative enterprise, which could be disrupted, distorted, or frustrated even by so limited an intrusion as watching."

• • •

Theories of privacy as personhood, however, fail to elucidate what privacy is because the theories often do not articulate an adequate definition of personhood. Freund's notion of attributes irreducible in one's selfhood is far too vague, and merely substitutes "selfhood" for "personhood." Bloustein's discussion of personhood as "individuality" fails to define the scope or nature of individuality. Other commentators define personhood as a type of autonomy, but as Jed Rubenfeld observes, "to call an individual 'autonomous' is simply another way of saying that he is morally free, and to say that the right to privacy protects freedom adds little to our understanding of the doctrine."

Personhood theories are also too broad. Our personalities are not purely private; indeed, there is much that is unique to the self that we readily display and express in public. An artistic work is often an expression of the deepest recesses of an artist's existence; yet art is rarely exclusively a private affair. Gavison, for example, criticizes Bloustein's dignity conception because "there are ways to offend dignity and personality that have nothing to do with privacy." She elaborates: "Having to beg or sell one's body in order to survive are serious affronts to dignity, but do not appear to involve loss of privacy."

Further, theories of privacy as personhood tell us why we value privacy (to protect individuality, dignity, and autonomy), but their usual focus on limiting state intervention in our decisions often gives too little attention to the private sector. Merely restricting state interference is not always sufficient to protect privacy. Therefore, beyond an account of where the state ought to leave individuals alone, personhood theories frequently fail to explain how personhood is to be protected. This is essentially what Gross and O'Brien are claiming when they criticize Bloustein for telling us only why we value privacy rather than what privacy is.

b. Antitotalitarianism

In his influential article, The Right of Privacy, Jed Rubenfeld ... argues, "[b]y conceiving of the conduct that it purports to protect as 'essential to the individual's identity,' personhood inadvertently reintroduces into privacy analysis the very premise of the invidious uses of state power it seeks to overcome." When the state endeavors to protect personhood, it must adopt and enforce its own conception of individual identity, impinging upon the freedom of individuals to define what is central to their identities for themselves.

Rubenfeld offers an alternative conception, defining the right to privacy as "the fundamental freedom not to have one's life too totally determined by a progressively more normalizing state." Rubenfeld claims that privacy protects against a

"creeping totalitarianism, an unarmed occupation of individuals' lives." Privacy "is to be invoked only where the government threatens to take over or occupy our lives—to exert its power in some way over the totality of our lives." As Rubenfeld elaborates, "[t]he anti-totalitarian right to privacy ... prevents the state from imposing on individuals a defined identity."

Although Rubenfeld's critique of the personhood conception is certainly warranted, he fails in his attempt to abandon a personhood conception. If privacy concerns only those exercises of state power that threaten the "totality of our lives," then it is difficult to conceive of anything that would be protected. Indeed, as Rubenfeld himself notes, infringements on privacy are "creeping," that is, they often occur in small encroachments into our private lives. As I explain in depth in another article, privacy is often destroyed by an aggregation of these minor encroachments, not always by a large exercise of state power.

Rubenfeld's critique of personhood forbids him to sketch any conception of identity that the law should protect, for to do so would be to seize from individuals their right to define themselves. By abandoning any attempt to define a conception of identity, Rubenfeld's conception of privacy collapses into a vague right to be let alone. To the extent it tells us anything meaningful about which exercises of state power must be curtailed, it must depend upon an affirmative conception of personhood. For example, Rubenfeld states: "[C]hildbearing, marriage, and the assumption of a specific sexual identity are undertakings that go on for years, define roles, direct activities, operate on or even create intense emotional relations, enlist the body, inform values, and in sum substantially shape the totality of a person's daily life and consciousness." Rubenfeld defines these aspects of life as at the heart of identity because of their pervasiveness and longevity. Thus, he is creating a conception of personhood that focuses on pervasiveness and longevity as the defining factors.

Rubenfeld is correct that laws purporting to be protective of personhood can impose a view of what aspects of life are essential to the individual and hence supplant the individual's own self-definition. However, Rubenfeld is too quick to condemn as "invidious" all state power that shapes identities. Not all such exercises of state power are pernicious. In fact, privacy is both a positive and negative right; it is not just a freedom from the state, but a duty of the state to protect certain matters via property rights, tort law, criminal law, and other legal devices. Without protection against rape, assault, trespass, collection of personal information, and so on, we would have little privacy and scant space or security to engage in self-definition. To preserve people's ability to engage in self-definition, the state must actively intervene to curtail the power of customs and norms that constrain freedom. Therefore, although Rubenfeld is correct that the state cannot be neutral when it becomes involved in one's self-definition, he errs in assuming that he can develop his theory of antitotalitarianism without an account of personhood.

6. Intimacy

An increasingly popular theory understands privacy as a form of intimacy. This theory appropriately recognizes that privacy is not just essential to individual self-creation, but also to human relationships. As Daniel Farber correctly notes, one virtue of privacy as intimacy is that it "expand[s] moral personhood beyond simple rational autonomy." The theory views privacy as consisting of some form of limited access or control, and it locates the value of privacy in the development of personal relationships.

We form relationships with differing degrees of intimacy and self-revelation, and we value privacy so that we can maintain the desired levels of intimacy for each of

our varied relationships. For example, political scientist Robert Gerstein claims that "intimate relationships simply could not exist if we did not continue to insist on privacy for them." As Jeffrey Rosen observes: "In order to flourish, the intimate relationships on which true knowledge of another person depends need space as well as time: sanctuaries from the gaze of the crowd in which slow mutual self-disclosure is possible." By focusing on the relationship-oriented value of privacy, the theory of privacy as intimacy attempts to define what aspects of life we should be able to restrict access to, or what information we should be able to control or keep secret.

In *Privacy, Intimacy, and Isolation*, philosopher Julie Inness advances an intimacy conception of privacy: ... Privacy is "the state of the agent having control over decisions concerning matters that draw their meaning and value from the agent's love, caring, or liking. These decisions cover choices on the agent's part about access to herself, the dissemination of information about herself, and her actions."

Charles Fried, who understands privacy as control over information, advances an intimacy conception to locate the value of privacy and circumscribe the scope of information over which we should have control. For Fried, "[i]ntimacy is the sharing of information about one's actions, beliefs or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love." Similarly, James Rachels contends that privacy is valuable because "there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people."

How is "intimate" information to be defined? For Fried and Rachels, intimate information is that which individuals want to reveal only to a few other people. Philosopher Jeff Reiman critiques Fried and Rachels for claiming that intimate information is merely scarce information that individuals want to keep away from others. He argues that Fried and Rachels's view of intimacy "overlooks the fact that what constitutes intimacy is not merely the sharing of otherwise withheld information, but the context of caring which makes the sharing of personal information significant." The ability to love and to care for others transcends the mere sharing of secrets. For example, Reiman states that "[o]ne ordinarily reveals information to one's psychoanalyst that one might hesitate to reveal to a friend or lover. That hardly means one has an intimate relationship with the analyst." "What is missing," Reiman declares, "is that particular kind of caring that makes a relationship not just personal but intimate." ...

Tom Gerety also bases his formulation of privacy on intimacy. Beginning with the criticism that existing theories of privacy are far too broad because they lack any meaningful limitation in scope, he goes on to claim that "[i]ntimacy is the chief restricting concept in the definition of privacy." Intimacy is "the consciousness of the mind in its access to its own and other bodies and minds, insofar, at least, as these are generally or specifically secluded from the access of the uninvited." In other words, his definition of intimacy is a form of limited access to the self. However, this definition fails for the same reasons the limited-access conceptions fail: it does not adequately provide us with a scope and content to privacy. Gerety attempts to develop his definition of intimacy a bit further, discussing it later in his essay in terms of its expressiveness of individual identity and autonomy. He thus claims that abortion is a private decision because it is "an intimate one, expressive of both [a woman's] identity and her autonomy."

But Gerety's intimacy theory of privacy, like the theories he critiques, is too broad. Gerety attempts to limit privacy with the terms "identity" and "autonomy," but

these are very broad terms that could apply to almost every action or decision an individual undertakes. ...

On the other hand, privacy-as-intimacy theories are too narrow because they focus too exclusively on interpersonal relationships and the particular feelings engendered by them. Although trust, love, and intimacy are facilitated by privacy, these are not the sole ends of privacy. As DeCew points out, information about our finances is private yet not intimate. Trust, love, and caring are not broad enough to comprise a conception of privacy; although privacy helps us achieve these ends, these ends do not comprise a complete conception of privacy. As Farber notes, there are many sexual relationships devoid of love, liking, or caring as there are many acts expressive of love, liking, or caring (such as buying gifts) that are not considered intimate.

Furthermore, privacy's value does not lie exclusively in the development of intimate human relationships. Intimacy captures the dimension of the private life that consists of close relationships with others; but it does not capture the dimension of private life that is devoted to the self alone. As Weinstein observes:

> [T]here is a wide range of instances where to speak of something as private is not to imply intimacy. Individuals not intimately related may nevertheless assert that their relation or activity is a private one in the sense that it is not the proper concern of the community or some institution, such as the state, a church, or a business firm.

For example, as political scientist Priscilla Regan notes, computer databases pose a significant threat to privacy but "do not primarily affect ... relationships of friendship, love, and trust. Instead, these threats come from private and governmental organizations—the police, welfare agencies, credit agencies, banks, and employers."

In sum, privacy-as-intimacy conceptions can be too broad if they do not adequately define the scope of "intimacy." Most often, however, such conceptions are too narrow because they exclude many matters that do not involve loving and caring relationships.

Helen Nissenbaum, "Contextual Integrity Up and Down the Data Food Chain"

(2019) 20:1 Theo Inq L 221

A. CI Fundamentals: Four Theses

According to the theory of contextual integrity (CI), privacy, defined as CI, is preserved when information flows generated by an action or practice conform to legitimate contextual informational norms; it is violated when they are breached. To elaborate this definition, this Article characterizes the theory of contextual integrity (CI) in terms of four fundamental theses, each an incremental progression from the one before. These theses convey the substantive assertions of CI, while providing a vehicle for comparing CI to other conceptions, definitions, and theories.

1. Thesis 1: Privacy is the Appropriate Flow of Personal Information

This thesis acknowledges the critical importance of information about persons as fuel for a robust social sphere. There is nothing wrong with sharing or gathering information about ourselves and others; there is no presumption in favor of hoarding, holding, or stopping flow. The theory of contextual integrity (CI) does not

valorize information containment. Privacy as contextual integrity does not accept the implications of other definitions that identify privacy with no flow, with stoppage, secrecy, and data minimization. It does not agree that when Alice and Bob are talking, Eve always violates their privacy. It does not identify data leakage as a privacy harm, or any collection as privacy violation. CI cares only whether the flow is *appropriate*, not whether it takes place at all.

Flow plays such an important role in the articulation of contextual integrity that it deserves its own paragraph. I chose flow to serve as a neutral term to refer to the passage or transmission of information or data from party (or parties) to party (or parties). Each of the alternative terms I considered, such as share, collect, disseminate, distribute, transmit, receive, or communicate, was richer in meaning than flow, and their augmented meanings bundle assumptions that theory requires be made explicit.

Thesis 1 gives CI an important strategic advantage over definitions of privacy as secrecy, which, in my view, imperil privacy's moral standing. Although privacy as secrecy, or stoppage of flow, provides clarity to the concept, its legitimate scope is extremely narrow. How many times have we heard people announce that privacy must be balanced against—insert your favorite alternative—security, efficiency, convenience, usability, functionality, commercial profit, public health, etc., or the generic version, "trade privacy for utility!"? What these people almost always mean is that information must flow in order to support security, convenience, and so on, thus implicitly adopting a definition of privacy as stoppage of flows. If privacy were stoppage, or secrecy, it would stand to reason that more often than not it would need to be traded off against other useful, socially valuable exchanges. But, as contextual integrity, privacy allows for information flows that are appropriate, including flows needed to promote utility—i.e., security, convenience, and the like.

2. Thesis 2: Appropriate Flows Conform with Contextual Informational Norms ("Privacy Norms")

Thesis 1 leaves open the question of what it means for flows to be appropriate. To answer, Thesis 2 introduces the construct of contextual informational norms that express or characterize information flows. Building on the work of social theorists and philosophers, this construct presumes a conception of social life not as an undifferentiated whole, but as constituted by distinct social contexts. Although these works posit differing logics and labels—spheres, realms, fields, institutions, domains—nevertheless, they share a view of society as constituted by diverse domains. CI takes on board some of the common insights without committing to any specific one of these theories. With the general term *context* CI connects with neighboring theories, while also drawing on intuitive understandings of distinct social domains and even quite common societal arrangements, such as law and policy in the contemporary United States, which acknowledges these differing domains with differing bodies of law for distinct spheres of engagement and respective institutions, including, for example, commercial, constitutional, family, financial, workplace, and health. As noted, although contextual integrity is committed to differentiated social space, it is tied neither to any one theoretical account nor to any one paradigmatic society.

In assuming that society comprises multiple social spheres, CI does not commit to a particular set or arrangement of spheres and allows for different societies (historical eras, cultures, etc.) to comprise different ones. It does, however, conceive of a particular structural arrangement, including several key contextual constituents. These include roles or capacities in which people act; paradigmatic activities and

practices; and respective ontologies. They may also include paradigmatic institutions and venues. Physicians, physical therapists, and patients; physical examinations, blood tests, and treatment; and symptoms, insurance forms, illnesses, diagnoses, and medications; hospitals, ambulances, and physicians' offices are among the constitutive elements of the healthcare context, just as teachers, students, reading, writing, studying, schools, and universities partially constitute education.

In the past, I had not placed sufficient emphasis on functions, purposes (goals, ends), and values around which contexts are oriented. I would like to make up for this prior lapse by saying that these—let's call them teleological—factors define the very essence of a respective social context. Even though, or perhaps because, they are the most important aspects of social contexts, they frequently are the most contentious, debated, and controversial aspects. We may agree that among the defining aims of healthcare are alleviating pain, preventing contagion, or curing disease, but we may disagree over whether prevention is more important than cure, prolonging individual life more important than average population health, and so forth. Some have argued that healthcare values include equity, the provision of care (or organs for transplants) according to need, irrespective of ability to pay; others disagree. Some hold that physicians should respect whatever paths patients choose; others insist that physicians have a right and duty to steer. Although, from the beginning, teleology has been a steady part of CI, experience has shown that it is frequently overlooked. Social contexts are what they are because of respective contextual aims, purposes, and values.

One caution is to avoid thinking of contexts in spatial terms, although, admittedly, standard usage allows for both spatial and non-spatial meanings. Respective roles, activities, purposes, information types do not exist in a context; rather, these factors *constitute* a context. Although certain places are generally associated with respective contexts—hospitals, schools, department stores, churches, governors' mansions—they do not, by themselves, define a context.

We have mentioned roles, practices, goals, and values but not yet contextual informational norms, a fundamental building block of contextual integrity. Though we now turn to them, space constraints require that we do so with great brevity and insufficient detail. Consider the term *norm* to have a meaning close to the term *rule*, and social or societal norms to be norms that govern individuals insofar as they are members of societies. The reason for preferring *norm* to *rule* is the former's flexibility. While rules tend to be explicit and emanate from authoritative sources, norms may be explicit or implicit, may emanate from a variety of sources, may or may not be enshrined in law, may be commanded or merely emergent, may vary over time and across cultures, may be strict or approximate, may be universally or merely locally known, and so forth. I apply the term *contextual norm* to norms that describe, prescribe, proscribe, and establish expectations for characteristic contextual behaviors and practices.

As an empirically or historically discoverable sociological matter, contextual norms can be finely or coarsely grained and finely or coarsely tuned. In certain situations, such as a court of law, behaviors are finely governed by norms (and rules), whereas in others, such as a social event, they may be quite nonspecific. In general, because the existence of norms shapes people's expectations, behaviors or practices that contravene them are commonly met with surprise, shame, anger, or even punishment.

Among contextual norms are those that govern information flows. Thesis 2 asserts that information flows are judged appropriate insofar as they conform to, or at least do not contravene, these norms. The presence of norms may explain, for

example, why one feels angry or disappointed when a good friend reveals to others the details of one's troubled marriage, why we do not ask coworkers (even friends) about their salaries, or why we assume that our votes in a democratic election are not known by government officials. Nonetheless, constituents expect the voting patterns of their political representatives to be available to them, clients expect lawyers to share their educational credentials, the Internal Revenue Service requires citizens to reveal earnings, and building owners expect tenants to provide details of their financial standing. *Notice: Although the last four involve information sharing, none of them involve tradeoffs of privacy because the flows are appropriate*.

Thesis 2 differentiates CI from procedural approaches to privacy, such as "notice and choice," ubiquitous in the contemporary digital landscape of websites, social platforms, mobile systems, and apps. They are procedural because no matter what the substance of the practice, as long as subjects are notified and are allowed either to refuse or consent, privacy has been duly respected. I have argued that the original *Code of Fair Information Practice Principles* is largely procedural, exhorting information collectors to follow prescribed steps in their bid for "fair" practices. Although Thesis 2 does not rule out procedural constraints, it stands by the idea that substantive, normative dos and don'ts define appropriate flows.

A word on terminology: Going forward, I use the shorter term *privacy norm* interchangeably with *contextual informational norm*.

3. Thesis 3: Five Parameters Define Privacy (Contextual Informational) Norms: Subject, Sender, Recipient, Information Type, and Transmission Principle

Thesis 3 asserts that fully articulated contextual informational norms prescribe flows in terms of (actors) who sent the information, who received it, about whom it is, what types of information are involved, and constraints imposed on them (transmission principles). To ascertain whether an action or a practice respects privacy, values for all five parameters must be specified in order to map resulting flows onto governing norms. The comparative template that CI provides has, arguably, served as one of its most successful contributions, for it effectively reveals changes to which other approaches are blind. Thus, defenders of a video-cam may reject complaints because video subjects are "in public" and can be seen by anyone passing by. CI reveals, at the very least, that a transmission principle has changed—reciprocity—for no longer is it possible for subjects to see those who see them. Similarly, the "no change" defense of public records (including court records) rendered digitally and placed online ("public is public") can be challenged by carefully comparing the five parameters before (paper records in courthouses) and after (digital records, available online).

Several points are worth noting, both to elaborate on Thesis 3 and to reveal the line it draws between CI and other approaches. First, values for actor and information-type parameters are identified in terms of respective contextual ontologies. Subjects, senders, and recipients are described in their contextual roles, that is, are acting in capacities drawn from contextual ontologies, whether physician, teacher, elected politician, priest, customer, police officer, investor, friend, or congregant. Information likewise is conceptualized according to contextual ontologies, whether symptoms, medications, grades, voting records, demographics, salary, social security number, or church donations.

Second, evidence supports the fidelity of contextual informational norms to privacy expectations. One source is U.S. regulation where a close analysis of privacy rules for financial and health information, following passage of the Gram-Leach-Bliley

Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA), respectively, revealed the presence of CI's five parameters. This suggests that where precision is needed relevant parameters are not overlooked. A second source is direct empirical scientific study of people's expressed privacy expectations, including results from two large factorial vignette studies which not only demonstrated that people have a refined appreciation of all five parameters, but reinforced the proposition that descriptions of information practices that do not cover all the parameters are ambiguous and may be interpreted in different ways by different people.

Third, many have found the transmission principle (TP) parameter to be puzzling because, on its face, it is less familiar to accounts of privacy than actor-capacities and information types. A closer look reveals that TPs do perform a decisive function in other accounts, and definitely in law and policy, but are not explicitly recognized as such. Recognizing transmission principles as a distinct dimension of privacy norms has given CI a richer set of variables with which to characterize data flows in privacy-relevant ways.

Transmission principles are quickly demystified once one considers common instances, such as consent. No-one following privacy is unfamiliar with subject-consent, but conceived as a TP within a norm, its action is to condition the flow of information from sender to recipient on the consent of the information subject. Beyond consent, the possibilities for constraints that may serve as TPs are endless. Although some are more salient than others, such as, "with notice," "entitled," "required by law," "coerced," "reciprocal," "in confidence," "buy," and "sell," TPs are structurally generative. Take consent. The most commonly assumed is subject's consent, but it need not be so; consent may be required from parents or other legal guardians and may be either necessary or sufficient, or both. Authorization is similarly generative as to both the authorizing parties and the conditions that need to be met. The 4th Amendment of the US Constitution is a case in point, requiring "a warrant," meaning authorization from a judge provided on condition of showing "probable cause."

Fourth, Thesis 3 challenges privacy truisms that generally hold sway in public debates, research, and approaches to public opinion polls: a) challenging the dichotomy of public/private data and positing, instead, the promotion of a multiplicity of information types reflecting contextual ontologies; b) challenging accounts that hang privacy status on only one factor, e.g., subject control, or whether the information is "sensitive," instead maintaining a simultaneous focus on all parameters (In the Cambridge Analytica scandal, for example, it was not only that subject consent was bypassed; outrage focused on Cambridge Analytica as an unacceptable recipient of the data that were gathered by Facebook.); c) challenging the chokehold of subject control as the sole arbiter of privacy, instead highlighting alternative TPs.

Fifth, and lastly, CI requires that values for *all five* parameters be specified. As argued above, failing to do so results in an incomplete and ambiguous account of information flows. However, because working with five independent parameters is demanding, certain circumstances may justify a reduction. For example, in a healthcare context, it is usually safe to assume that the data subject is the patient, in education, the subject is a student, etc. Or, in developing an app for specific needs where one can count on a closed set of values for one or more of the parameters, one may fix others; for example, if the app is for use among friends, one might justifiably settle on subject consent (or subject control) as the universal TP. Or, in an access control system built for use in a hospital the number of norm permutations that need to be considered can be controlled, since the context and circumstances of use impose natural limits on the variety of actors and information types for

which it must account. Finally, within carefully defined settings, it might even make sense to bundle information into two categories, enabling different constraints for each. Thus, information about mental disorders may be judged more sensitive than most other medical conditions and fewer known parties may have access, under more restrictive conditions. The circumstances in which such reductions are justified nevertheless call for vigilance, particularly to stay true to the assumptions about context of study and use.

4. Thesis 4: The Ethical Legitimacy of Privacy Norms is Evaluated in Terms of: A) Interests of Affected Parties, B) Ethical and Political Values, and C) Contextual Functions, Purposes, and Values

The CI narrative proceeds as follows: Social life is thick with flows of personal information, which may and sometimes may not conform with entrenched contextual informational norms. A practice violates a privacy norm if resulting flows fail to map onto expected values for the parameters. Consider, hypothetically, if the U.S. Census Bureau were to share raw data with the Immigration and Naturalization Service, or if a priest were to divulge a congregant's confession to a third party. In such cases, CI would hold that a *prima facie* violation of contextual integrity has occurred, but would not necessarily cease evaluation at that point. Always resisting practices that violate entrenched norms would make CI an exceedingly conservative theory and would be exceedingly problematic for two reasons. One is that CI is designed to respond to the challenges of rapidly evolving sociotechnical practices and many novel flows may be highly beneficial. The other is that intransigence in the face of change sets CI as a descriptive theory, with no capacity to evaluate—either entrenched norms or contravening principles.

The approach outlined in *Privacy in Context* remains conservative, but instead of flatly rejecting novel flows, it presumptively favors entrenched norms, simultaneously offering a process for adjudicating between the two. To begin, evaluators follow the approach laid out in CI for pinpointing changes, followed by a three-layered comparative analysis to locate respective strengths and weaknesses. Based on these findings, the evaluator recommends in favor of either the status quo or the challenger on grounds of moral quality.

According to Thesis 4, the first two layers are a) interests and b) ethical and political values, both unsurprising to anyone following the privacy debates. Public deliberations surrounding law and policy pay great heed to asking familiar questions. For a given information practice, who wins and loses? Whose preferences and interests are served; whose are not? What are the costs, what are the benefits? While economic arguments often downplay the interests of data subjects, privacy advocates have highlighted harms to subjects from data exposure, such as identity theft and embarrassment. In the literature, researchers have pointed to longer-term threats and subtler harms, such as helplessness, shrinking self-determination, losses of power, boundary control, and the reduced ability to modulate relationships. Beyond the interests of affected parties, there are many who have focused on the ethical and political values at stake, going back to the U.S. drafters of the FIPPS, who sought to level the playing field for the owners and controllers of information systems and the subjects of these systems. To critics, it was not merely that decision makers learning facts about you could harm your prospects (i.e., your interests), but they could be acting against your interests unfairly and unjustly. Privacy advocates defended the connections between privacy and ethical and political ends about which there was broad agreement—freedom of speech and thought, political freedom, and autonomy.

Layer c) of Thesis 4 introduces a distinctively contextual consideration. Influenced by Priscilla Regan's groundbreaking work on the social value of privacy, CI requires that information practices be evaluated in terms of contextual functions, purposes, and values. Let us return to the healthcare context where, for centuries, medical professionals have sworn to the secrecy of their patients' health conditions. Confronting the risks of information technologies and pressures to share information, privacy advocates have warned against inadequate protections, citing harms of discrimination, shame and embarrassment, reduced employment opportunity, and so forth. These are all good reasons to ensure that healthcare professionals honor the obligations of entrenched privacy norms to keep patient information out of the grasp of, say, advertisers, prospective employers, curious onlookers, or the press.

As convincing as these warnings are, a dispassionate analyst would proceed to weigh the interests of patients against others whose interests are affected by flows of health information, for example, prospective employers seeking to hire candidates with the best health prospects, marketers seeking promising customers for a new drug, or even users of a dating site wanting the most robust partners. For many privacy debates, this is the battleground; sleeves are rolled up and fervent arguments weigh in favor of one or the other side. For CI, however, missing from these debates is a critical consideration, namely contextual purposes and values. Beyond stakeholder interests, analysts must seek constraints on information flow that promote the goals and values of the healthcare context. This argument proceeds as follows: if patients are fearful that medical information will flow to the wrong parties, they may lie to their physicians, hop from doctor to doctor, or not seek medical advice at all. So doing, they place not only their health at risk, but the health of others, thereby undermining contextual purposes.

Contextual purposes and values sometimes may disfavor the data subject's interests, even in the healthcare context. Having advanced in our understanding of environmental health hazards and communicable diseases, CI may support overriding individual patient interests or preferences in favor of onward sharing of information with others, for example, public health officials. This would allow information to be aggregated and analyzed, hazards (toxic chemicals or restaurants with poor hygiene practices) to be pinpointed, and the further spread of disease contained. Similar lines of reasoning support adherence to privacy norms for other contexts, e.g., student privacy, or voter privacy, in support of contextual ends, not only to secure respective interests.

In the years since the first comprehensive account of CI was published in *Privacy in Context*, the theory has confronted important questions. Relevant to Thesis 4 is a question about recommended steps for evaluating the moral legitimacy of entrenched norms. According to the book's narrative, when established, normative practices confront competing, novel, disruptive sociotechnical practices, the analysis that ensues compares the two in terms of the three-layer criteria. In presenting CI to various audiences, I have come to appreciate the innumerable, unprecedented practices and associated data flows that defy any easy comparison with preexisting practice that may serve as reasonable precursors or counterpoints. It turns out that although the advantage of having a clear counterpoint is being able to choose the better performer, in fact, conducting an evaluation, as described in Thesis 4, does not require locating a reasonable counterpoint as a first step. An analysis that first carefully maps out data flows in terms of the five parameters and then proceeds to consider interests, societal values, and contextual ends and values may provide sufficient insight to reveal the moral legitimacy or moral hazard of a given practice.

B. CI General Highlights

Before concluding Part One, I offer a few concluding remarks. First, again as regards why CI begins a comparative evaluation with a presumption favoring entrenched norms, this conservative stance relates to the choice of appropriateness, not correctness or excellence, as the initial entry point. Appropriateness suggests a balance, already a societal compromise. It deserves utmost protection not because it favors the interests of individual subjects above all others, or the opposite, but because it already represents a settled accommodation of diverse interests as well as societal and contextual ends. I have favored entrenched norms, presuming that they reflect a settled accommodation. Critical theorists may chide me; at best, this is a naïve ideal, a fiction. The starker reality is that practices are entrenched because they are favored by society's powerful, the entitled. If this is so, my hope is that the clear-eyed pursuit of CI's evaluative analysis is as likely as any to reveal the tyranny of convention at the same time as it reveals the delicate balance of multiple conflicting interests and plurality of values that complex constraints on flow seek to realize.

The cascade of four theses allows for stops along the way. One may, for example, subscribe to Thesis 1, but not the rest; Theses 1 and 2, but neither 3 nor 4. And so on. Worth noting are the challenges to Thesis 3, asserting that the set of five parameters is incorrect or incomplete. I'd like to highlight one version of this challenge, posed by Anupam Datta, an important collaborator whose work formalizing CI significantly sharpened it. Datta has urged the inclusion of a use parameter, noting the frequency with which use is cited as a factor in the U.S. legal domain, importantly, in HIPAA and GLBA privacy rules. I am increasingly persuaded that adding a use parameter might, after all, be a necessary antidote to a policy environment in which data holdings may be obtained through unimpeded company takeovers even when data flow between the companies in question may be heavily conditioned, or even prohibited.

CI opens the door to privacy regulation and design that is, at once, more nuanced as well as more precise. Resistance to regulation frequently is framed as fear of overly blunt regulation—all or nothing, yes-flow or no-flow. Because five parameters provide five dimensions of variation, regulation can be precisely tailored to need. Regulators can consider restricting recipients, or articulating particular fields of information, or can adjust transmission principles (as discussed above) with significant sensitivity. Similar strategies work for system design as well. Turning to CI, technology developers with ambitions to promote privacy-by-design could ensure that the languages they choose to express the rules governing data flow have sufficient expressive power to embed multiple variables. Formal language experts are beginning to offer such languages and associated logics.

Ignacio Cofone & Adriana Z Robertson, "Privacy Harms"

(2018) 69:4 Hastings LJ 1039

I. The Problem of Privacy Loss

A. Normative Concepts of Privacy

Judith Jarvis Thomson famously observed that "[p]erhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is." In the forty years since she made this observation, the literature has made little

progress on this front. Helen Nissenbaum, accordingly, has noted that "[o]ne point on which there seems to be near-unanimous agreement is that privacy is a messy and complex subject." Robert Post has gone even further, remarking that "[p]rivacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."

Daniel Solove, for example, has identified no less than six distinct ways to conceptualize privacy: as (1) the right to be let alone, (2) autonomy or the limited access to the self, (3) secrecy or concealment of discreditable information, (4) control over one's personal information, (5) personhood and preservation of one's dignity, and (6) intimacy and the promotion of relationships. While this classification is widely accepted, it is not universal. Across these different normative conceptions, the term "privacy" typically refers to the control of one's personal information, or as limiting access to such information. More recently, scholars have begun to adopt a conception of privacy that centers around the contextual integrity of personal information.

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

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

Posner, on the other hand, famously argued that privacy is mainly a matter of concealing undesirable facts about oneself. This concealment can take two forms. First, an individual can hide unflattering information about herself: information that would lower the receiver's opinion of her. For example, concealing the fact that one has been convicted of a crime. An individual can also conceal information by a second, more subtle means, by failing to correct a misunderstanding or misperception. For example, she might prefer not to divulge a serious health problem to an employer. With respect to this second type of concealment, Posner adds that an individual might choose to reveal information selectively without strictly lying or deceiving, and that individuals are always eager to disclose facts that portray them in a positive light. In short, a fair evaluation of Posner's conception of privacy is that it exists mainly as a device to deceive: to create or maintain a false impression.

In contrast, some view privacy as simply control over one's personal information. A refined notion of an individual's level of privacy, they argue, shows that privacy is not the absence of information about her in public (as in Posner), but

rather the control that she has over that information. Privacy has also been defined along these lines as the absence of undocumented personal knowledge.

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

Finally, supporters of privacy as intimacy argue that the concept of intimacy encompasses all the types of information that an individual would rather keep private. They see privacy is a tool to protect the individual from being subject to misrepresentations that could occur when others know some pieces of information about her out of context, which could lead to misunderstandings. The right to privacy defines information territories: places where it is socially acceptable to keep or to disclose information, and which define the boundaries of private life and social life.

B. Descriptive Concepts of Privacy

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

The normative approach leads to two difficulties. First, it ignores the basic intuition that "privacy" depends on both facts (including cultural, historical and technological facts) and context, not only on some essential characteristic. Second, many of the concepts that are used to define privacy are themselves hard to pin down. While these can be useful for linking privacy breaches to situations that people intuitively consider wrongful, their primary contribution is not to provide a sharp boundary. For example, autonomy and personhood have many facets and are no easier to define than privacy itself. Someone suffering from a privacy violation might complain that such violation injures her personhood or autonomy, but this statement does little to pin down the circumstances under which an individual loses privacy. These difficulties are so acute that Post has argued that it is extremely difficult, if not impossible, to succeed in this endeavor of defining the right to privacy's essence.

In contrast to the six normative conceptions of privacy, we can think of three descriptive conceptions of privacy: limiting access to personal information, control over information, and appropriate information flows. Because these views aim to identify when privacy is diminished, rather than when privacy rights are breached, they relate more closely to identifying harms to privacy. The discussion above makes clear that one way to interpret the perspective of those who advocate for privacy as the right to be let alone or for privacy as secrecy is that they operate under a logic of access, while we can see most of the proponents of privacy as autonomy or as control as operating under the logic of control, and most of those

who view privacy as personhood and intimacy doing so based on a logic of information flows. As we discuss in more detail below, our model can be interpreted in light of any of these three descriptive conceptions of privacy.

Rather than aiming to define privacy, we offer a functional model of privacy that is designed for legal analysis. While our proposal is compatible with these previous approaches, our goal is to develop a model that is both simple to apply and useful for legal analysis. As Ryan Calo has said, "describing the outer boundaries and core properties of privacy harm helps to reveal values, identify and address new problems, and guard against dilution." In the following Part, we aim to describe such boundaries. We do so with a model that captures the idea that information privacy is about people's ability to deduce our personal information, which underlies each of the three descriptive approaches to privacy discussed above.

Woodrow Hartzog, "What Is Privacy? That's the Wrong Question"

(2021) 88:7 U Chicago L Rev 1677

Every year on the first day of my course on information privacy law, I ask my students to define the concept of privacy. Usually, I get a few different answers, each of which is built around some singular and definitive conceptualization of privacy. Some notions include: Privacy is "control over personal information." Privacy is "secrecy." Privacy is the "right to be left alone." And so on. Then I gently push back, asking my students about notions of privacy that fall outside their definition. Which definition should the law adopt? All of these definitions seem right, yet somehow not enough. I ask whether it is a good idea to define privacy so broadly that it is synonymous with all personal interference. My goal is for students to appreciate that there are many ways to conceptualize privacy, each of which is underinclusive or overinclusive. I point to the many ways that scholars have explored various components of the important but remarkably vague notion of privacy, happy to leave its definitive boundaries undefined. Scholars and lawmakers are not always so comfortable with such uncertainty; I have made my peace.

Throughout history, privacy has evaded a precise meaning. Initially, lawmakers had no compelling need to give the concept a singular legal definition. The earliest personal information and surveillance rules and frameworks for privacy leveraged specific concepts such as solitude, confidentiality, and substantive due process. But after Samuel Warren and future-Justice Louis Brandeis called for a "right to privacy" in 1890, the concept took on new life as a term of art in legal frameworks. Plaintiffs in tort cases were asked to articulate the private nature of facts and actions. Judges confronted with the argument that the state had violated a defendant's Fourth Amendment rights were asked to determine whether the defendant had a "reasonable expectation of privacy" in the activity or space that the state had invaded. State and federal legislators created numerous statutes that sought to protect "private" information from exposure. In short, from the early 1900s to the present day, lawmakers and judges have regularly been compelled to give the term "privacy" a broad and consistent legal meaning. It hasn't gone well.

Daniel Solove, the John Marshall Harlan Research Professor of Law at the George Washington University Law School and perhaps the most prominent and influential privacy scholar of our day, wrote at the turn of the millennium that privacy was "a concept in disarray." In his foundational book *Understanding Privacy*, Solove noted

that people have defined privacy in many different ways, including "freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations." In the twentieth century, privacy theorists seemed intent on crafting a definitive, singular meaning for privacy. Alan Westin wrote that "[p]rivacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Charles Fried similarly argued that "[p]rivacy ... is the *control* we have over information about ourselves." Ernest Van Den Haag wrote that "[p]rivacy *is* the exclusive access of a person (or other legal entity) to a realm of his own." Some of these theories defined privacy in service of autonomy. Others characterized privacy through its service of intimacy or dignity.

But it turns out that a broad and singular conceptualization of privacy is unhelpful for legal purposes. It guides lawmakers toward vague, overinclusive, and underinclusive rules. It allows industry to appear to serve a limited notion of privacy while leaving people vulnerable when companies and people threaten notions of privacy that fall outside the narrow definition. And it often causes people who discuss privacy in social and political settings to talk past each other because they don't share the same notion of privacy.

The chaos and futility of competing conceptualizations of privacy is why Daniel Solove's research on privacy has been so important and influential for our modern privacy predicament. In an ongoing series of articles and books starting in 2001, Solove worked to reshape the entire narrative around privacy by suggesting that we stop obsessing over what privacy is and start asking what privacy is for. To Solove, there is no singular common denominator of privacy. Scholars seeking it are destined to spin their wheels for eternity. "Privacy is not one thing," Solove wrote, "but a cluster of many distinct yet related things." Taking inspiration from Ludwig Wittgenstein's concept of family resemblances, Solove argued that privacy is best thought of as an umbrella term that brings together a group of concepts that "draw from a common pool of similar characteristics."

Solove's work in privacy has been extraordinarily influential for scholars, policymakers, and practitioners. His works are regularly invoked to counter the argument that privacy is important only to people with "something to hide." Solove's response is that privacy isn't just about hiding things. Solove keenly understands the central role that narratives and stories play in our understanding of privacy. He presciently argued that the modern privacy predicament involving industry's large-scale data processing efforts is more akin to Josef K.'s byzantine bureaucratic nightmare described by Franz Kafka in *The Trial* than the dystopian universal surveillance described by George Orwell in *Nineteen Eighty-Four*. Solove argued that automated systems fueled by personal data don't just power surveillance tools. These tools power systems that make decisions about people's personal lives. They control and obscure, leaving people frustrated and vulnerable. Much of Solove's work, such as my collaborations with him regarding the Federal Trade Commission's regulation and enforcement of privacy, aims to make sense of tumultuous areas involving the law of personal information.

Perhaps most importantly, Solove's work provides a structure that frees scholars and lawmakers of the burden of finding one, singular notion of privacy to rule them all. He also helped shepherd in the algorithmic turn in privacy scholarship, which opened the door for discussions of how privacy issues impact marginalized and vulnerable populations. There are many virtues to understanding privacy as a pluralistic, fluid concept. Such an ideal furthers diverse values and is capable of having both intrinsic and utilitarian worth and coexisting with many different policy goals.

Under this notion, people in politics, commerce, and society can work to solve complex information problems without constantly relitigating privacy's meaning.

Instead of squabbling over the binary boundaries of privacy, people who understand privacy as more of a vague umbrella term can leave the line-drawing question for another day and get to work identifying problems created by specific conduct, articulating the values implicated by those problems, and crafting solutions to the problems that serve those values. Starting in the late 1990s, Solove, along with other pioneering scholars such as Anita Allen, Danielle Citron, Julie Cohen, Helen Nissenbaum, Neil Richards, Joel Reidenberg, Paul Schwartz, and others—responded to the late-century ossification of privacy law with new insights for a world gone digital. They arrived not a moment too soon.

The world has never seen anything like the power held and used by modern technology companies. It has never been easier to surveil people and collect, store, search, analyze, and share their personal information. The fair information practices (FIPs), a set of principles developed in response to the risks created by electronic databases, are not enough to meet the moment. Regulatory manifestations of the FIPs such as the European Union's General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and California's Consumer Privacy Act (CCPA) seek transparency and accountability from companies and control for people over their own data. They are the closest thing the world has to a "common language for privacy."

Most of our modern data privacy rules, however, are built to serve individualistic notions of privacy—that is, to respect a person's autonomy and dignity. Few are aimed at disrupting power disparities between people and companies, protecting individuals from harassment and manipulation, or seeking a collective wellbeing for a diverse population in which many people, including women, people of color, members of the LGBTQ+ community, and others, are particularly vulnerable to information systems. If lawmakers were tied to the notion of privacy as control over personal information, they might struggle to diagnose the problem as anything beyond a lack of adherence to fair information practices. Regulators might just engage in extreme FIPs enforcement in the hope that the companies will eventually reach full transparency and that people will have full command over how their data is processed. Companies would go along because the FIPs do little to interfere with business models built around exploiting data.

Transparency, consent, and control solutions won't be enough to get us out of this mess. First, as Solove has noted, the "privacy self-management" approach embodied by notice and choice regimes puts the onus on individuals to protect themselves. But the massive scale and widespread adoption of digital technology have made meaningful informational self-determination impossible. People are simply overwhelmed by the choices presented to them. The result is a threadbare accountability framework that launders risk by foisting it on people who have no practical alternative to clicking the "I Agree" button. Second, consent and control are a poor fit for certain information problems, like manipulation and harassment, that have little to do with how information is processed and more to do with how mediated environments put people at risk. Finally, seeking to give people control over their personal information doesn't account for collective, societal harms from personal information technologies. Privacy exists for groups and communities, too. Your data can put other people at risk in ways that are hard to predict. We're going to need richer, more diverse notions of privacy to solve these problems.

Thankfully, people have been hard at work converting privacy from a blunt tool into a Swiss Army knife, with each prong in service of a different value or purpose. Scholars have proposed a remarkable array of ways to think and talk about different

notions of privacy, including intellectual privacy, sexual privacy, quantitative privacy, and more. They have built out conceptualizations of privacy as obscurity, trust, power, privilege, security, safety, procedural due process, a civil or human right, and the contextual integrity of information flows. They have argued that privacy protects democracy, "the processes of play and experimentation," identity, the incomputable self, and significantly more. When lawmakers and judges accept privacy as a concept that contains multitudes, each of these different notions can explicitly be brought to bear on the real needs of people, groups, and institutions rather than deploying an ill-fitting theory in diverse contexts.

Lawmakers have started to embrace privacy as a concept with multiple overlapping dimensions. Legislators and regulators have begun to target problems such as nonconsensual pornography, microtargeting, manipulative user interfaces, and automated decision-making with innovative rules leveraging secondary liability for dangerous and abusive design choices, substantive limits on data collection and use, relational duties of loyalty and care, equitable relief, and criminal penalties in addition to implementing outright bans on particular technologies.

Judges are also evolving in their thinking about privacy. For years, courts have struggled mightily trying to figure out what it means to have a "reasonable expectation of privacy." Too often, that translates to things not exposed to others. But that has changed a little recently, as in *Carpenter v United States*, in which a majority of the U.S. Supreme Court conceived of privacy as dependent upon several different factors such as the scope of exposure and the nature of the information.

By getting us past the threshold question of what privacy is, Solove's work provides room for scholars and lawmakers to tackle bigger phenomena, such as how capitalistic incentives cause companies to leverage information in harmful ways, how the design of information technologies matters just as much as data practices, and how marginalized populations are affected first and hardest by privacy-invasive actors. Solove is a pragmatist, and, as such, his work consciously looks at the nature of privacy-related problems. This focus also helps elevate the importance of scholarship aimed at the last legal mile of privacy solutions: how privacy harms are mitigated through legislation, regulation, and litigation. Solove's own work with Danielle Citron on privacy and data security harms provides a map for judges and lawmakers to better articulate what harms result from bad information practices and which remedies are best to address those harms.

The year is 2021, and privacy is still a concept in disarray. But that's okay. There is now too much data that is collected by too many different entities and used in too many different ways for any singular definition of privacy to be legally useful anyway. Daniel Solove's work on understanding privacy has imposed order upon chaos, shifting our focus away from questions about what privacy is and toward the different problems we want our privacy-based rules to address and the specific values we want them to serve.

NOTES AND COMMENTS

1. It is worth reflecting on how the theories mapped by Solove relate to each other. First, how does the "limited-access conception" of privacy differ from solitude? Consider the distinctions mentioned in Solove's text. Second, how does the "limited-access conception" of privacy connect to the "secrecy" conception? Third, identify one way the two theories complement each other and one way they diverge. Fourth, compare the theories of "privacy as control over personal information" and "privacy as intimacy." What shared assumptions about privacy do they have, and how does each theory address the role of relationships differently? Theories of privacy as "intimacy" and "personhood" both emphasize human dignity and

autonomy. Fifth, do these theories differ in their focus on individual relationships versus societal or state dynamics? Sixth, the text suggests that the "limited access" and "intimacy" conceptions both involve choices about what to reveal or withhold. How do these choices depend on social context?

2. How does thesis 1 of "Contextual Integrity" (redefining the concept of privacy) compare with older notions of privacy, such as secrecy? Does this redefinition provide an advantage over the six concepts outlined by Solove? Thesis 2 of "Contextual Integrity" introduces the idea of contextual informational norms. How do these norms differ from procedural privacy approaches like "notice and choice," and why are they important for determining appropriate information flows? How does the contextual integrity theory account for the possibility that entrenched norms may reflect the interests of the powerful rather than a balance of diverse societal interests?

3. The five parameters of contextual informational norms (thesis 3) propose a framework for assessing privacy. Do the contextual integrity parameters address the public–private information dichotomy differently than the six concepts outlined by Solove? In thesis 4, contextual integrity uses three layers (interests, ethical/political values, and contextual purposes) to evaluate the ethical legitimacy of privacy norms. What role do these layers play in how the framework addresses the relationship between public and private information?

4. How would you relate Solove's general approach resulting in his six-concept classification and Nissenbaum's general approach to defining privacy resulting in the mapping of privacy as secrecy, privacy as control, and privacy as contextual integrity? Do you see a difference in their mapping approaches?

5. Why is "What is privacy?" the wrong question according to Hartzog? Do Solove and Nissenbaum fall into the pitfalls that he identifies in their classifications? The text argues that seeking a singular, universal definition of privacy is unhelpful, but it also mentions various ways privacy can be conceptualized (e.g., intellectual privacy, sexual privacy). Why does embracing privacy's multidimensionality help lawmakers and judges address diverse privacy problems? Hartzog suggests focusing on what privacy is *for* rather than what privacy *is*. In your opinion, does this perspective affect privacy lawmaking?

6. The concept of data ownership is often discussed in conversations about privacy. Which concept or concepts of privacy do you think it builds on? Does that say anything about its potential advantages and disadvantages?