

Who Gives a 'Tweet' about Privacy?

Prepared by Christopher Parsons*

May 10, 2009

* Doctoral student in the University of Victoria's Political Science department. Comments welcome, and can be directed to Christopher@Christopher-Parsons.com

Table of Contents

Unauthorized Capture and Transmission of Data	3
Twitter and Statutory Notions of Privacy.....	5
Claims to Privacy	5
From a Claim to Statutory Norms.....	7
Twitter and Privacy in Social Context.....	9
Privacy, Society, and Citizen-Solidarity.....	9
Contextualizing Privacy in Public	11
An Actionable Account of Privacy for Public Spaces.....	12
A Problem-Based Account	13
Towards an Expectation of Privacy on Twitter	14
New Technologies, New Problems, and Contesting New Norms.....	15

Can individuals who publicly disclose information about themselves in digital environments reasonably believe that their statements are somehow private? Scott McNealy, CEO of Sun Microsystems, would likely argue they cannot. McNealy is well known for uttering the phrase, “Privacy is dead, get over it.” His comment captures the attitude that individuals ought to expect software and hardware to extensively track, analyze, and store data about individuals’ increasingly virtualized lives. While neither data monitoring or retention are new occurrences, digital technologies have extended the capacity of individuals and groups to capture and digest vast quantities of data in cost-efficient ways. The current insistences that third-parties should have access to consumer data using freely accessible Application Programming Interfaces (APIs) to produce data mash-ups, accompanied by consumers’ expectations that personalized services be delivered at low costs, might lead us to wonder whether it is somewhat absurd for individuals to expect for their online disclosures of personal data to be seen as private. If we understand ‘privacy’ as ‘restricting access to consumer data’ then implementing strong privacy safeguards would seem to limit the new services that consumers gain access to, and thus run counter to their consumer interests. The difficulty, of course, is that such a response to our opening question avoids clearly defining what a “reasonable” expectation to privacy is. Furthermore, it adopts a notion that privacy matters to the individuated consumer, instead of society more broadly. Thus, we might rearticulate our opening question, asking “what might constitute a reasonable expectation to privacy in a public space, and how would such an expectation carry over into digital environments such as social networks, blogs, and messaging clients?”

This paper engages with this question at a conceptual, rather than empirical, level. As such, I consider various understandings of ‘what is privacy’ to determine the benefits and drawbacks of adopting a tort-based claim to privacy, as well as statu-

tory rights, social, contextual, and taxonomic understandings of privacy. I will examine these understandings against the recent phenomenon of people publishing the minutia of their daily lives on Twitter, a social networking and microblogging service. Such a focus will let me contribute insights from academic privacy literature to discussions of whether privacy has a place in Twitter, and hopefully assist in nuancing privacy discussions about Twitter. Does Twitter's user-base have a reasonable expectation to privacy, even when disclosing elements of their life in public, and if so what might condition these expectations?

Before responding to these questions, however, a brief description of Twitter is in order, as well as a brief sketch of why I think talking about privacy and Twitter in the same sentence is warranted. Twitter lets users post comments up to 140 characters to a localized user space at Twitter.com (e.g. twitter.com/BrentSpiner). The service, very generally, bears strong resemblance to Short Message Services (SMS) that are built into most cellular carriers' networks, but differs insofar as most messages, or 'tweets', are published publicly.¹ Anyone can view, read, and archive these tweets and yet, even in this intentionally public social networking environment, privacy remains something near and dear to many Twitter users.. This concern or interest in privacy is evidenced when entering 'privacy' as a search term in Twitter search bar – thousand of hits turn up. *lusuzi* writes, "i really want some more privacy in life,"² *MightymightyBookworm* that s/he "is overall really annoyed with the internet due to a lack of privacy,"³ and *Carrie Valdez* asks if, "are we giving up our privacy? we are everywhere. Or will we too be desensitized to our own self-presentation?"⁴ Of course, while this search term may identify a host of tweets, we cannot assume that each user holds a similar conception of what is and isn't private. Nevertheless, the position that 'if you are in public, you should not hold an expectation of privacy' isn't a position held by all users of Twitter – privacy seems to be something that many claim to be concerned about.

To begin thinking through what an expectation to privacy on Twitter might be referred to, we will first turn the role of privacy torts as envisioned by Warren and Brandeis. Their focus on tort damages and tort-related definition of 'privacy' will lead us to question whether a privacy tort is genuinely needed to protect the individual, or if an extension of copyright law would alleviate many of the worries facing Warren and Brandeis. We then shift from tort law to examine privacy as an individualistic claim through the lens of Westin, and how Simitis insists that such a claim must be understood within a wider social context. Westin's dependence on sensory fields

¹ There are two exceptions to these public posts, which are not discussed at length in the paper. First, individuals can 'lock' their profiles to let them control who can view their tweets. Second, members of the message service can send direct messages, which are delivered to particular individuals and not placed in a public 'tweet stream', or listing or public messages. Both of these prevent the general public from seeing tweets, and are outside of this paper's question, 'should individuals who publicly communicate in digital environments hold a reasonable expectation to privacy?'

² Comment available at: <http://twitter.com/lusuzi/status/1692473573>

³ Comment available at: <http://twitter.com/keepitraw/status/1691726883>

⁴ Comment available at: <http://twitter.com/toxicgerl/status/1691908592>

will leave us with questions of how effective his approach is in a digital environment characterized by a *lack* of sensory awareness, and Simitis' focus on controlling individual data poses problems for integrating data control into contemporary web-based ecosystems. Nevertheless, the social character of privacy holds promise, which will see us turn to Regan. She builds on Simitis' argument that privacy is critical for healthy democracies, but her association of seclusion and citizen-solidarity will lead us to ask whether Twitter itself thus constitutes a danger for the contemporary nation-state.

To explicitly understand the negotiation of privacy claims, we conclude by turning to Helen Nissenbaum and Daniel Solove. Nissenbaum will insist that those who speak in public *do* have a reasonable expectation to privacy and focuses on the need to understand the norms surrounding particular discussions and broadcasts in environments such as Twitter. Unfortunately, her focus on conservative normative understandings and lack of clarity surrounding the constitution of these understandings leaves it unclear how we can establish a cohesive account of what is and isn't a reasonable expectation of privacy. With this deficiency in mind, we turn to Daniel Solove's taxonomic account of privacy, which reveals the benefits of adopting a problem-based approach to privacy that can be used to clarify what are, and are not, reasonable expectations of privacy. Ultimately, from this examination of privacy literature and its evaluation against Twitter we will find that while Solove's account is preferred, even it raises questions of who should be involved in constituting social norms, with the implicit suggestion that privacy scholars must extend beyond problems alone to broadly engage with discussions concerning the politics of identity and norm foundation as well as philosophies of law and justice.

Unauthorized Capture and Transmission of Data

Almost every cellular phone that is now sold has a camera of some sort embedded in it. The potential for individuals to capture and transmit images without permission has become a common fact of contemporary Western life, but this attitude has not always existed. When Polaroid cameras were new and used to capture images of indiscretions for gossip columns, Warren and Brandeis wrote an article asserting that the unauthorized capture and transmission of photos and gossip constituted a privacy violation. Such transmissions threatened to destroy "at once robustness of thought and delicacy of feeling. No enthusiasm can flourish, no generous impulse can survive under [gossip's] blighting influence" (Warren and Brandeis 1984: 77). Individuals must be able to expect that certain matters will be kept private, even when exhibited in public spaces – it must be recognized that they have a right to be let alone – or else society will deviate from its progress towards civilization.

The right to be left alone means that publications must avoid inappropriately intruding on the private lives of individuals, and that these publications secure the consent of individuals prior to disclosing information collected about them (Warren and Brandeis 1984: 79). Warren and Brandeis maintain that intrusions be limited on two grounds. First, per the principle of inviolate personality there should be no reproduction of one's physical and mental actions that would hinder a person's abil-

ity to live with dignity. Any unauthorized retransmission of personal affairs will lead a person to normalize their behavior, to be less like the really are, and thus condition their behavior by dimming their enthusiasm and generosity. Furthermore, intrusions must be limited because they may cause serious moral or reputational damages, and such damages should be protected against (Warren and Brandeis 1984: 78). Tort law should be used to defend against these damages, and entitle individuals to recourse when damage is incurred. Rather than just focusing on physical injuries, tort law should be reformed to take emotional duress into account.

While the authors speak of an individual's 'inviolate personality', we might ask whether they are making a privacy claim, or instead are making claims that expand the jurisdiction of copyright and tort-damages under the auspice of privacy. Privacy in public spaces, under a copyright/expanded damages reading, would mean that reproductions of personal thoughts and actions without consent (barring cases of legitimate public interest and lowered expectations of attention resultant from holding public office) or libel gossip could be prosecuted. At the same time, however, Warren and Brandeis note that 'public' disclosures (e.g. court proceedings) can be disclosed to the citizenry without infringing on an individual's privacy. Thus, there is a distinction between being in public (i.e. walking down the street) and being in the public eye (i.e. in court). We might understand this distinction in the sense that what legally enters the public domain (in copyright terms) cannot be considered as violating one's privacy, even if it includes deeply embarrassing facts that are of minimal value to a court proceeding. When the state's eye forces you onto the record an embarrassment, rather than privacy violation, is felt per Brandeis and Warren's account.

What would this mean for public digital environments such as Twitter? Would publishing minutia in 140 characters and seeing that minutia republished in a gossip column constitute a 'privacy violation'? What if someone who is not on a user's friends list 'retweets', or reposts, the message to all of their friends without informing you that they are doing this? It would seem that such a rebroadcast of personal information, if damaging, would constitute a privacy violation even though Twitter is, in part, *designed* to encourage and facilitate such sharing. At the same time, however, if what is republished is not emotionally or reputationally damaging (e.g. reposting a tweet with your phone number and picture) would this constitute a privacy invasion? Given that a violation being registered depends on the individual both learning of the publication and having a negative reaction to it, if neither of these conditions are met then while dignity might be damaged it is questionable whether the felt effects of such damage would be sufficient to drive a successful tort claim.

A stronger argument might be made that when a tweet is reposted without a user's consent that a copyright infringement takes place.⁵ Of course, such an argument

⁵ For an interesting discussion of copyright and Twiter, I would refer you to Jonathan Bailey's post 'Copyright and Twitter', located at <http://www.blogherald.com/2008/05/05/copyright-and-twitter>.

rests on an assumption that text in online environments retains standard copyright and that we can clearly state what tweets merit copyright protection and which do not. Even making a case for fair dealing is challenging. In the case of Twitter what constitutes fair dealing – a portion of a 140 character message, the entirety of a twitter stream, or some other allocation of text? Should infringement occur when someone profits on my words without compensating me, or do I lose the legal claim to profits because the words are spoken in public? While asking these sorts of questions tends to terrify copyright experts, there are grounds under which copyright infringement can be understood and used within a court of law. Making an argument on these grounds would leverage a vast body of law and could address lost earnings or damages that follow from someone inappropriately retweeting a post/making public a private communication. On this basis, it is unclear why, exactly, Warren and Brandeis need a privacy tort when laws for liable speech and copyright can already address sullied reputations and loss of profits from the republication of thoughts and ideas.

Twitter and Statutory Notions of Privacy

Whereas Warren and Brandeis explicitly built a tort claim to privacy (and can be read as *implicitly* laying the groundwork for a right to privacy), theorists such as Alan Westin attempt to justify a claim to privacy that would operate as the bedrock for a right to privacy. Spiros Simitis recognizes this claim, but argues that privacy should be read as both an individual *and* a social issue. The question that arises is whether or not these writers' respective understandings of privacy capture the normative expectations of speaking in a public space, such as Twitter; do their understandings of intrusion/data capture recognize the complexities of speaking in public spaces *and* provide a reasonable expectation of privacy that reflects people's interests to keep private some, but not all, of the discussions they have in public?

Claims to Privacy

Westin asserts that 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” (Westin 1970: 7). Each relationship is judged on its own merits, with individuals potentially providing different information to their various communicative partners. Within the range of social relationships that individuals are immersed in there are ongoing adjustments to ‘balance’ one’s sociality and reclusiveness. Westin argues that claims to balancing sociality and reclusiveness are manifest throughout the natural world, from relationships between wild animals, to primitive societies, to contemporary human societies. While there are differences in the particular instantiations of privacy norms in each human society, such norms are broadly captured across all societies as:

1. Individual and group norms.
2. Norms that differentiate between privacy and the total absence of other presences.

3. Normative understandings of what constitute appropriate curiosity for understanding reality and appropriate degrees of surveillance for maintaining social order.
4. Norms that demonstrate increasingly sophisticated expectations of anonymity that correspond with the shift from thick to thin social bonds.

The common mode of realizing when a privacy claim is being contested is when an individual experiences an unwarranted or undesired intrusion on their sensory fields (Westin 1970: 30). Such intrusions occur when they unsuccessfully try to make one of the claims listed below, and instead find themselves subject to forced disclosure(s) of personal facts, to intrusive surveillance, or to having their communications republished without first giving their consent. The claims to privacy that are made include:

1. Solitude – where individuals try to separate themselves from their social group.
2. Intimacy – where they act in small groups to experience mental release.
3. Anonymity – where individuals enter large groups without providing their identity to engage in self-reflection in a space free of surveillance and identification.
4. Psychic reserve – where they limit communications with others to provide a claim to privacy even in an intense relationship.

Individuals and organizations alike make these four claims, and each is subject to the aforementioned modes of intrusion. Within a public domain, we might expect to enjoy intimacy by secluding a group from the larger public (e.g. a table in a bar), anonymity by crossing into a digital space using a pseudonym to learn and reflect on choices, and psychic reserve by not disclosing our full life-history in a public space, such as a grocery store. In terms of a public communicative space, what would it mean to enjoy privacy when using Twitter?

Presumably, members of such public environments would *not* be attempting to seclude themselves from others. They could be engaging in an intimate conversation similar to a discussion in a bar and, given the high noise-to-signal ratio, they might have an expectation of talking without likely being unduly disturbed or surveyed. Despite this hope for intimacy, however, Twitter emphasizes sharing/reposting other people's comments, which makes it dubious that an unwarranted republication/retweeting would constitute a substantive infringement on an intimacy-based claim to privacy. At the same time, we might wonder if it is possible for an individual to realize another party is paying more attention to a conversation occurring in public than is socially acceptable *without* them retweeting a comment.

Without full recourse to the sensory fields that we have depended on to notice contestations of our claims to privacy, we may not register moments of identification and surveillance though, per Westin's categories identification and surveillance, such attention would infringe on claims to anonymity. While Westin is trying to carve out a claim or right to privacy (he asserts a claim at the beginning of the text,

but this claim seems to shift towards a right to privacy in the third chapter) grounded in historical and anthropological evidence, we are left wondering how exactly we would register a challenge to a privacy claim where our centuries-honed senses are of minimal assistance in determining whether someone has breached our fields. Ultimately, while Westin does note what conditions we would base a reasonable expectation of privacy on, we are left without a clear idea of how to recognize when our expectations are not being met in a digital communicative domain such as Twitter. His work seems well suited for developing a statutory claim to privacy, but less suited for digitized public environments where identifying privacy breaches is largely possible only when another person engages with the norms of the same environment (i.e. retweeting another person's tweet).

From a Claim to Statutory Norms

Turning to Simitis, a former German data protection commissioner, we can learn how a regulator may want to instantiate Westin's claim to privacy in law. By approaching privacy as the right to control one's personal data, Simitis transforms the issue from an abstract theoretical argument that is true across time to one that is better "aware of the political and social background" motivating privacy debates (Simitis 1987:709). Privacy is not only something of value to the individual, but is critical to healthy democracies as well. To contextualize the contemporary privacy discussion, he notes three differences born of technology that separate contemporary privacy discussions from those of Warren and Brandeis.

1. Privacy considerations express conflicts affecting everyone, not just individuals.
2. Exceptionally high-quality surveillance has become normal.
3. Personal information is increasingly used to enforce standards of behavior (Simitis 1987: 709-10).

Simitis focuses on the exchange of personal information as the source of privacy problems and, as a result of behavioral analysis and vast data gathering instruments, whole populations are now targeted instead of just specific individuals. In the face of this vast data collection assemblage, privacy violations can be limited by establishing regulatory controls which govern how and why personal information is disseminated (Simitis 1987: 737). Given the capacity of government and business alike to shape citizens' interests, and Simitis' concern that such shaping undermines individuals' abilities to independently make decisions and take actions (Simitis 1987: 733), we would expect him to agree with Daniel Solove's argument that a set of data points can be used to develop the equivalent of a digital Seurat painting, with the individual citizen as the painting's subject. Unlike Solove, however, Simitis is working from the position that sufficient regulation along with an independent data commissioner can limit the free-flowing retransmission of personal data and thus limit who can legitimately generate such digital paintings. A strong regulatory body with the following characteristics must be established if individuals' privacy is to be secured. Further, such a body will mitigate infringements on citizens' constitutional

rights and thus shield the nation-state's constitutional foundations from damages. The regulatory body must:

1. Recognize the unique nature of personal information.
2. Ensure that data collectors explicitly note what collected personal data will be used for.
3. Interpret existing regulations fluidly and can quickly develop new regulations in order to keep up with changes in technology.
4. Operate independently of the legislature and be able to rapidly respond to data transmission and retention problems.

In terms of speaking in public, when surveillance assemblages capture personal data and transmit it automatically there is a danger the social actors will regulate their actions in accordance with popular norms, thus stymieing the growth or maintenance of the democratic state. While a network such as Twitter does recognize that individuals 'control' their own data, it is now an accepted norm of the Internet that web spiders from major search engines categorize particular pages based on their apparent content and keywords. Contextualized advertising systems may inspect tweets to identify keywords and deliver advertisements based on those words. In both of these cases, there is a collection/observation of personal data accompanied by a transmission of elements of that data to a foreign server. As a result of categorizing the web content it is possible that a particular group of people may be more likely to find your tweets, or delivered particular advertising. In both cases it is possible, and common, for spiders and advertising systems to misidentify keywords, miscategorize web content, and potentially embarrass individuals based on the categories their content is found in and the advertising delivered alongside their content. In the face of these 'risks' should data collectors be required to clearly note what any collected data will be used for and, if so, how is this notification performed? Is agreeing to an End User License Agreement (EULA) sufficient to waive your privacy claims in relation to particular third-party data collection and use? These are the kinds of questions that Simitis' regulatory body would be pressed to engage with.

Furthermore, do individuals have a reasonable expectation to privacy over the entirety of what they tweet, or only on particularly revealing tweets that clearly contain personal data? If someone tweets "loving Ouch," this is practically meaningless unless a data collector can associate 'Ouch' with the DJ N-Dubz. At the same time, "feeling lost after my abortion" is both revealing, arguably addresses a very personal matter, and could be used to injure the person's reputation if the information were captured, analyzed, and transmitted in inappropriate ways. Given the vast quantities of information divulged in public discourse on Twitter, what heuristic would effectively identify personal information versus noise? How could a regulatory body hope to monitor the enormous amount of personal data that is placed online every day and how individuals and groups subsequently survey and analyze the data?

Effectively, the challenge with Westin's claim to privacy and Simitis' regulatory instantiation of it is that privacy becomes something that we have and is affected by

the outside – surveillance ‘takes away’ one’s privacy and it is up to a data regulator to limit how much privacy an individual loses. Further, these regulators are expected to identify appropriate reparations when invasions have taken place, both to compensate the individual and to associate costs with infringements or violations of core democratic rights.

We are left wondering, however, whether capturing personal information without any intent to use it to damage a person’s reputation – data may just be collected as part of a data accumulation project (e.g. the Internet Archive) – constitutes an infringement on an individual’s privacy. Given the sheer quantity of surveillance instruments that watch what individuals do in Cyberspace’s virtualized hallways, and these instruments’ key role in structuring digital environments, should we be quick to restructure the very foundation of how the ‘net has evolved to facilitate the ownership or control of personal space and data? Given the norms of digital networks such as Twitter, which emphasize sharing and collective knowledge development, is a control metaphor accompanied by a strong regulatory body well suited for developing a ‘reasonable expectation of privacy’ in Cyberspace? I would suggest that they are not, at least not as presented by these texts and as applied to some social networking spaces. As we will see in subsequent sections, contextualized understandings of social relationships and privacy norms facilitate nuanced understandings of what individuals expect to remain private online – the challenge for theorists such as Nissenbaum will be translating these insights into actionable principles and guidelines that data and privacy commissioners can use to perform their tasks.

Twitter and Privacy in Social Context

Simitis recognizes privacy as an issue concerning all of society. As a consequence, his position on the topic is differentiated from those of Westin, Warren, and Brandeis by asserting that privacy is essential for establishing and maintaining constitutional infrastructures. In this section, we take up the ‘social’ element of privacy, exploring it in more depth and to consider its role in establishing citizen-solidarity. In addition, we consider privacy as a contextualized norm that attaches different expectations of privacy to particular situations and encounters. While social-contextual accounts establish reasonable expectations to privacy in public, our hopefulness surrounding these accounts wears thin because the selected scholars exhibit an under theorized conceptualization of how socio-contextual norms are established. Effectively, without an account of how socio-contextual norms are developed in pluralistic environments we are left with little understanding of how to read privacy norms in public spaces like Twitter. Thus, while understanding privacy as contextual integrity does establish reasonable expectations (note the plural) of privacy, the multiplicity of such instantiations renders such understandings of limited usefulness for juridical application in contemporary pluralistic nation-states.

Privacy, Society, and Citizen-Solidarity

Pricilla Regan, in *Legislating Privacy*, argues that it is challenging to address privacy-related problems when they are only recognized as individual, rather than individuals *and* social, issues. She argues that a social understanding of privacy is needed to

recognize the breadth of data collection (similar to Simitis), and wants to shift privacy discussions from the language of 'balancing' individual and social interests to ones about competing societal interests. Modifying these discussions to recognize privacy's social value is intended to provoke nuanced understandings of privacy's roles in contemporary democracies, and readjust the stance that privacy should be sacrificed at the alter for security and market efficiency.

Regan's position rests on three pillars, two normative and one economic. Normatively, privacy is a common value because all individuals have some interest in privacy. Further, privacy retains a public value because it lets individuals limit personal disclosures and thus facilitates citizen-solidarity; too much personal disclosure would upset citizens' capacities to identify with one another as similar rights and duties holders (Regan 1995: 222-223). Economically, privacy operates as a collective, or non-divisible, economic good – it cannot actually be 'allocated' to individuals as products like candy bars, and consequently cannot be understood as just an individual's personal issue (Regan 1995: 223-224).

While she is situating privacy as a common value, Regan does recognize the value of individual claims to privacy (intimacy, seclusion, anonymity, etc) but her focus on the social lets her avoid advocating for any particular claim or understanding of individualist privacy expectations. She isn't saying the privacy is *just* a social value; it still retains value for particular individuals and there is merit in examining how and why individuals value privacy (Regan 1995: 213). Given that individuals uniformly hold *some* position towards privacy, she argues that it is a commonly held (though differently realized) value. It also has a public value insofar as it facilitates a reflective and independent body of citizens. It is essential that each citizen "can at some points separate himself from the pressures and conformities of collective life" (Emerson 1970: 546, referenced by Regan 1995: 225). Such withdrawals are helpful not only for developing thoughtful modes of political engagement, but also to promote citizen-solidarity. According to Regan, the more that we know about one another the less we perceive commonalities between us – privacy, or seclusion from the other, lets us avoid endangering social stability by learning too much about each other (Regan 1995: 227). In terms of economic norms, privacy is a collective good because it cannot be divided, nor can individuals be excluded from receiving privacy as a 'good' when laws, rights, and regulations are passed. Based on these three pillars privacy must be read as shared social good.

With these pillars in mind, we might wonder what it means for individuals to intentionally exhibit themselves in virtualized spaces such as Twitter. These communications environments rely on individuals to broadcast their particularities to maintain the services' business models – does participation in Twitter, where individuals demonstrates their particularities at the expense of seclusion, threaten to upset the communicative fabric stitching nation-states together? While we might think that this is preposterous, given that a minority of any nation's population actively uses Twitter, suppose we abstract slightly and image that a nation-state's entire population decides to tweet on a regular basis. Does such a mass public broadcasting of

personal data undermine the privacy that individuals require for a functioning democracy? If this is the case, then should services such as Twitter be regulated to secure the continuing legacy of the nation-state and limit public broadcasts of personal data?

Both of these questions appear somewhat absurd on their face, but do suggest a few things. First, the relationship between seclusion and citizen-solidarity as presented is problematic and likely needs to be adjusted or softened. Second, it appears as though there should be a distinction between mandatory and voluntary disclosures of personal data – seclusion must be something *available* to individuals and not something they are *obligated* to engage in. Thus, the ‘danger’ that public communicative environments would infringe on seclusion-related privacy is only realized if all discourse is forced onto public virtualized platforms. Barring this, Twitter does not seem to necessarily threaten either privacy at large or the continuing existence of the nation-state. At the same time, however, Regan’s discussion of privacy does articulate the need to situate expectations to privacy in terms of both the individual and society. The social environment that discussions occur in must be taken into account, as must the ‘classical’ understandings of individuals’ privacy discussed by theorists such as Warren and Brandeis and Westin.

Contextualizing Privacy in Public

Helen Nissenbaum would likely insist that citizen-solidarity (in terms of the privacy discussion) is only threatened when data is appropriated in violation of normative expectations that address how personal information should be appropriated and distributed. The former norm correlates with what is appropriate or fitting to reveal depends on context of the data collection – merely being in a public space does not mean that all information collections are appropriate (e.g. demanding to know a stranger’s name and not accepting ‘it’s none of your business’ as a response would be inappropriate, whereas giving one’s name to an employer would be appropriate) (Nissenbaum 2004: 120-121). The latter norm is meant to establish that there are some transmissions of personal data are acceptable and others that are not; while I might expect a public ‘tweet’ to be reposted on Twitter, I might not expect it to be transferred into a databank that is used to develop detailed consumer profiles.

Effectively, Nissenbaum is arguing that personal information is always ‘tagged’ with a particular context and that, as a result of contextualizing the norms governing data sharing environments, privacy is never wholly ‘up for grabs’. Instead, conservative social norms ought to govern what are appropriate data collections and transmissions of personal actions and conversations that take place in public. Moreover, given that the scope of these norms is internal to its context she is refusing to adopt an *a priori* understanding of what is and isn’t captured under the umbrella of privacy. What is considered private should “reflect norms of appropriateness and flow, and breaches of these norms are held to be violations of privacy” (Nissenbaum 2004: 127). While her theory of contextual integrity is universally applicable, its avoidance of prescribing what are private and public actions leaves it sensitive to different cultures, political systems, and nation-states.

On this account, expectations of privacy in public would reflect the culture's normative accounts of what are and are not appropriate collections and transmissions of data gathered in public environments. This may mean that a practice of broadly capturing the ethnicity of public transit users in a public database is acceptable in some contexts, and unacceptable in others. One of the difficulties facing this account of privacy in public, however, is that while Nissebaum thinks that conservative norms should guide what are and aren't appropriate norms we are left without a clear statement that identifies which groups are responsible for establishing these norms. Do legally actionable norms coagulate at the level of the nation-state, the city, the city block, the ethnic community, or somewhere else?

When we turn to reflect on discourse in public spaces such as Twitter, some of this ambiguity may fade away. In this environment, the technical design of the communications network suggests that other users can appropriate and retransmit tweets on the network. At the same time, however, with an open API and the widespread development of statistics software that is custom-built for Twitter, we might question whether the collection and storage of vast swaths of user data for analysis is an inappropriate transmission of data between first- and third-parties' databases. Does an open API mean that individuals ought to expect their conversations to be harvested, or instead should each person's understanding of a privacy norm be independently examined and evaluated? Adopting the latter position would seem to run contrary to most North American understandings of creating data sets and consumer profiles, but in cultures such as Germany that have strict requirements governing captures of personal data such a position more acceptable.

The global geography of Twitter, and similar digital systems, on the face of it presents a challenge to Nissebaum's theory given her lack of clarifying what and who is, and isn't, included in developing and identifying 'conservative' norms. In a multicultural, multiracial, multinational communicative environment with vast numbers of competing notions of what are reasonable expectations of privacy in public she has left us without a clearly defined system of either tabulating or adjudicating these claims. It will be as we turn to Daniel Solove's work, *Understanding Privacy*, that we will see an effort that accommodates the insights of Brandeis, Warren, and Westin, recognizes the need for privacy in a broad social context, while providing both a contextualized and actionable account to privacy.

An Actionable Account of Privacy for Public Spaces

To avoid particular instantiations of ethno-, anthro-, and polico-centrism in discussions of privacy discussion we saw Nissebaum introduce her notion of contextual integrity. While it failed to provide clear guidelines for identifying legitimate socio-political norms governing privacy claims, it did recognize that claims to privacy in public differed according the situation and actors involved. As we turn to Daniel Solove's work in *Understanding Privacy*, we see that he similarly wants to recognize the variability of privacy claims across cultures and societies. The taxonomy that he provides has the merit of establishing particular normative expectations of privacy while situating these expectations in an already existing legal framework.

Solove's taxonomy is based on an understanding of privacy *problems* – when do we experience an infringement on our privacy, and why do these experiences constitute an infringement? In the process of establishing his taxonomy he leaves open the possibility for additions to, or subtractions from, the particular privacy-related problems that he identifies. This leaves his taxonomy open to revisions based on different cultural expectations of privacy and their accompanied infringements. At the same time, however, Solove has grounded his taxonomy (primarily) in American experiences and the American legal system, which may leave us with concerns surrounding juridical conservatism.

Despite this concern we will find that, at a conceptual level, Solove's account both offers a nuanced understanding of what it means to expect privacy in 'public' virtualized environments, such as Twitter, while grounding his theory in practice. Solove offers a needed conceptual framework, leaves it open to modification and discursive intervention, and recognizes actionable principles; he 'gets' the complexities of digital social networking environments and offers us a way of recognizing reasonable expectations of privacy that can help us navigate social networks' turbulent digital seas.

A Problem-Based Account

Solove focuses on privacy violations, which are constituted by any activity that "causes problems that affect a private matter or activity" (Solove 2008: 102). Under his account, private matters are largely (though not entirely) shaped by particular cultures and histories (Solove 2008: 65). Broadly, there are four classifications of harmful activities, each with their own sub-violations:

1. Information collection – where individuals are subject to surveillance or interrogation.
2. Information processing – where records are aggregated, associated with discrete individuals, carelessly handled, used for purposes different than those consented to, and used for exclusionary purposes.
3. Information dissemination – where breaches of confidentiality occur, information is revealed to the harm of an individual's reputation, personal information is made widely available, blackmail becomes possible, a person's identity is assumed, or facts about a person distorted.
4. Invasion – where someone's tranquility or solitude is disturbed, or when there are incursions into a person's private decisions.

While these categories are meant to capture the range of possible violations, they avoid being *overly* contextual because this would limit a discussion of the violation beyond a specific situation. Solove recognizes that many of these violations, or problems, would typically be understood as problems for the individual but argues that while privacy rights and laws may protect individuals, this occurs "because it is in society's interest. Individual liberties should be justified *in terms of their social contribution*...The value of privacy does not emerge from each form or privacy itself but in the range of activities it protects" (Solove 2008: 173-4, emphasis added). 'Privacy problems', then, are instances where social norms are violated and where the soci-

ety may seek recourse to limit or prevent similar harms from being revisited upon its members.

Towards an Expectation of Privacy on Twitter

When we have been discussing ‘reasonable expectations of privacy’, it has been in reference to an approach that avoids reducing privacy to an unchanging essence. Instead, this position identifies a flexible normative account of when we can and cannot expect others to pay attention to, with ‘attention’ being understood to include data collection, processing, transmission, and so forth. The issue with such a broad understanding of this term is that “without a normative component to establish what society should recognize as privacy, the reasonable-expectations approach provides only a status report on existing privacy norms rather than guides us toward shaping privacy law and policy in the future” (Solove 2008: 73). Our account thus far has been dominated by *negative* rather than *positive* tests; what Solove’s taxonomy lets us do is exercise a method to develop normative understanding of what are privacy violations, from which we can explicate expectations of privacy.

To expand, a reasonable expectation of privacy assumes that there is a condition upon which we can determine what is and is not reasonable. Using Solove’s taxonomy and method, we can better understand what constitutes ‘reasonable’ expectations. Per his account, we expect that we will not be subject to unwarranted surveillance, not have our data handled carelessly, not have our personal data distorted, and so forth. The expectations that we might reasonably hold are found in the law, which establishes what is and isn’t legal, or what individuals can typically assume is and isn’t reasonable according to contemporary socio-juridical norms. At the same time, however, the openness of the law leaves space to recognize new expectations of privacy – by bringing interesting privacy-related cases to the courts, such as ones that evaluate an individual’s expectation to privacy in social networks, it is possible to reconfigure and rearticulate citizens’ reasonable expectations of privacy.

The danger with such an account, of course, is that there are times where expectations of privacy diverge from legal recognitions of privacy. Moreover, judges that are unaware of changing technical environments may make demands that are technically challenging or even impossible to comply with (e.g. requiring server operators to store IP address information when the servers and their software are designed to retain that data in the servers’ RAM rather than their hard drives). While such conservatism *is* a worry, and in this sense may be read to parallel the worries of conservatism accompanying Nissebaum’s account, Solove is at least establishing the ground for privacy norms *somewhere*. From this point we may disagree about the appropriateness of hearkening to the courts; perhaps we need to extend or alter who and what constitutes reasonable expectations, involve more bodies in the discourse of law, or reconfigure his baseline some other way. Such discussions are valuable, and critical to engage in, but doing so here would take us into discussions in philosophy of law and social and political accounts of norm generation. For our purposes, it is sufficient to simply note that using judicial decisions as the basis for normative account of privacy is not an uncontroversial point, and that Solove’s ac-

count would lead us into a range of surrounding literatures that address identity and norm generation.

Using Solove's taxonomy, and the reasonable expectations of privacy that emerge, we might examine whether users of Twitter have expectations of privacy when they tweet to one another. Is data being collected to blackmail an individual? Is the data a user is contributing to their twitter-stream being collected and distributed by third-parties without first securing the individual's consent of such collection and distribution? Is someone using a Twitter account to interrogate another person? Where the answers to these questions are 'yes', and where Solove's taxonomy derived from American law aligns with the legal expectations in an individuals' native land, the person's reasonable expectation to privacy have been violated. While Solove insists that an approach to privacy based on reasonable expectations to privacy is insufficient for establishing a comprehensive understanding of what privacy is, his own taxonomy lets us develop a juridically grounded set of conditions under which individuals might reasonably expect that their public communications should be understood as private. Such expectations would apply to physical and virtualized public discussions alike; members of Twitter have expectations to privacy that, unless otherwise contradicted in law, bear resemblance to those expectations individuals have in physically embodied public spaces.

New Technologies, New Problems, and Contesting New Norms

Texts that are central to the privacy literature regularly insist that new technologies extend the dimensions of the problems facing individuals and society. Many of these problems have been identified under the rubric of 'privacy'. There is a danger that in extending normative frameworks and broadening expectations of privacy that we may ignore other, better founded, paths to alleviate problems. Perhaps copyright, liable, and similar civil, criminal, and tort-based approaches may be better suited to resolve some problems than by using the language of privacy rights and claims. At the same time, where well-based, already existing, frameworks cannot effectively mitigate particular social ills resulting from data collection, analysis, and retransmission, we may want to enter these problems under the header of privacy. In the process, we may adopt a pragmatic taxonomy, such as Solove's, to understand the particular nature of the privacy claim.

Any such taxonomy, however, will fluctuate with the development of new technologies and their introduction into society. Widespread geo-tagging and facial recognition technologies that are integrated with consumer cameras, in combination with the ability to install firmware updates, greatly extend capabilities and potential problems associated with even familiar devices. Similarly, normative expectations to privacy fluctuate as social and cultural groups accept new members, new ideas, and new understandings of selfhood. On this basis, any theory of privacy is deeply implicated with norm-forming literature and must accommodate ever more nuanced understandings of how, when, and why norms can and do change, as well as how to react to such modulations in the domain of law.

At the same time, however, some technologies are extensions and enhancements of already existing social practices. Twitter is, arguably, an example of the public communicative sphere put on steroids – you can find a vast number of people to tweet with and exchange brief, sometimes intimate or informative, thoughts and personal details. Given that such behavior has close correlations with how people can behave in ‘meat’ space, they often expect that their notions of what are and aren’t acceptable privacy-related behavior on a public street or pub should carry over into a digital venue. If a legalistic approach to privacy norm formations is broadly adopted to clarify what these expectations ought to be, then they should vary with new juridical decisions concerning expectations of privacy in public. Privacy theorists would be well advised to critique the source and motivations for such understandings of norm creation, which will require them to engage with philosophers of law and justice. Their own accounts of how such norms are developed, in their efforts to establish inclusive and culturally sensitive understandings of privacy, can bridge privacy, legal, social, political, technological, anthropological, and philosophical literatures and thus both develop expansive understandings of how we might understand the term ‘privacy’ in various social contexts and bring attention to the value and need to interdisciplinary work to address some of society’s most complicated conceptual problems.

References

Nissenbaum, Helen (2004). "Privacy as Contextual Integrity," *Washington Law Review* Vol 79, No. 1, February 2004: 119-158.

Regan, Priscilla (1995). "Privacy and the Common Good" in *Legislating Privacy: Technology, Social Values and Public Policy*. University of North Carolina Press.

Simitis, Spiros (1987). "Reviewing Privacy in the Information Society," *University of Pennsylvania Law Review* 135: 707-46.

Solove, Daniel (2008). *Understanding Privacy*. Cambridge, Mass.: Harvard University Press.

Westin, Alan (1970). *Privacy and Freedom*. The Bodley Head, Ltd.

Warren, Samuel D. and Louis D. Brandeis (1984). "The right to privacy [The implicit made explicit]," in *Philosophical Dimensions of Privacy: An Anthology*, Ferdinand D. Schoeman (ed.). New York: Cambridge University Press.