

DRAFT

PRIVACY, VULNERABILITY, AND AFFORDANCE

Ryan Calo\*

February 23, 2017

A person without privacy is vulnerable. But what is it to be vulnerable? And what role does privacy or privacy law play in vulnerability?

This essay, adapted from the Clifford Symposium at DePaul University, begins to unpack the complex, sometimes contradictory relationship between privacy and vulnerability. I begin by exploring how the law conceives of vulnerability—essentially, as a binary status meriting special consideration where present. Recent literature recognizes vulnerability not as a status but as a state—a dynamic and manipulable condition that everyone experiences to different degrees and at different times.

I then discuss various ways in which vulnerability and privacy intersect. I introduce an analytic distinction between vulnerability *rendering*, i.e., making a person more vulnerable, and the *exploitation* of vulnerability whether manufactured or native. I also describe the relationship between privacy and vulnerability as a vicious or virtuous circle. The more vulnerable a person is, the less privacy they tend to enjoy; meanwhile, a lack of privacy opens the door to greater vulnerability and exploitation.

Privacy can protect against vulnerability but it can be invoked to engender it. I next describe how privacy supports the creation and exploitation of vulnerability in ways literal, rhetorical, and conceptual. An abuser may literally use privacy to hide his abuse from law enforcement. A legislature or group may invoke privacy rhetorically to justify discrimination, for instance, against the transgender individuals who wish to use the bathroom consistent with their gender identity.<sup>1</sup> And courts obscure vulnerability conceptually when they decide a case on the basis of privacy instead of the value that is more centrally at stake.

Finally, building on previous work, I offer James Gibson's theory of affordances as a theoretical lens by which to analyze the complex relationship that privacy mediates. Privacy understood as an affordance permits a more nuanced understanding of privacy and vulnerability and could perhaps lead to wiser privacy law and policy.

---

\* Assistant Professor, School of Law, Assistant Professor (by courtesy), Information School, University of Washington. The author would like to thank law professors Stephan Landsman, Paul Ohm, Julie Cohen, and other participants in the Clifford Symposium, editors at the DePaul Law Review, Scott Skinner-Thompson, and Evan Selinger for very helpful comments.

<sup>1</sup> These laws simultaneously compromise the privacy of transgender individuals. For an analysis, see Scott Skinner-Thompson, *Outing Privacy*, 110 Nw. U. L. Rev. 159 (2015).

## **Vulnerability**

Vulnerability refers to exposure to emotional, physical, or other negative forces. We can imagine being vulnerable to a positive force: a person could be vulnerable to a plea for help. But this seems to stretch the meaning of vulnerable. Usually when we refer to a person as vulnerable we mean vulnerable to harm.<sup>2</sup> A person or group who is invulnerable, of course, cannot be harmed or moved.<sup>3</sup>

In privacy and elsewhere, the law often conceives of vulnerability as the product of a status or a special relationship. A person with particular characteristics—for instance, a very young or old person—may be vulnerable to various harms and hence require greater protection. Privacy law reflects this view where, for instance, it protects children’s consumer privacy online but withdraws that protection at the age of 13.<sup>4</sup> In criminal law, the same action directed at a vulnerable victim may result in higher penalties under sentencing guidelines.<sup>5</sup> And of course most “undue influence” involves victims who are elderly or otherwise lack capacity.<sup>6</sup>

The law also sees vulnerabilities in certain relationships between people. In privacy, Jack Balkin has explored the idea that custodians of sensitive consumer information be considered “information fiduciaries,” complete with obligations of loyalty and care.<sup>7</sup> But generally a more narrow relationship is necessary to trigger these obligations. Thus, we understand subjects in an experiment to be vulnerable to the researcher and hence require special protections throughout and beyond the study. We also think of patients as vulnerable to doctors and lay clients as vulnerable to financial advisors.

---

<sup>2</sup> See Martha Albertson Fineman, *The Vulnerable Subject and the Responsive State*, 60 *Emory L.J.* 251 (2010).

<sup>3</sup> Perhaps they are not even a person. As philosopher Martha Nussbaum argues, a capacity to be vulnerable is in some sense critical to the human condition. On her account, a person who is entirely hardened against society and incapable of trust essentially ceases to be human. See Martha C. Nussbaum, *The Fragility of Goodness: Luck and Ethics in Greek Tragedy and Philosophy* (1986).

<sup>4</sup> Child Online Privacy Protection Act of 1998, 15 U.S.C. § 6501-6506.

<sup>5</sup> E.g., *Sentence of Imprisonment for Offenses Against Children, Elder Persons, or Handicapped Persons*, Haw. Rev. Stat. § 706-660.2.

<sup>6</sup> For a full if skeptical discussion of undue influence in the probate context, see Ray D. Madoff, *Unmasking Undue Influence*, 81 *Minn. L. Rev.* 571 (1997).

<sup>7</sup> Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 *U.C. Davis L. Rev.* 1183 (2016). Woodrow Hartzog and Neil Richards have explored related concepts such as a greater role for confidentiality in digital privacy and, more recently, the importance of promoting trust between firms and consumers. Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 *Stan. Tech. L. Rev.* \_\_ (forthcoming 2016).

This binary conception of vulnerability as either present or absent is hardly inevitable. We can imagine a more nuanced understanding that takes into account circumstance.<sup>8</sup> The legal literature is indeed replete with more nuanced discussions of vulnerability. For example, work by Florencia Luna conceives of vulnerability not as a label that applies or does not apply but as a layer of personhood. Thus, for Luna, the proper way to understand vulnerability “is not by thinking that someone *is* vulnerable, but by considering a particular situation that *makes or renders* someone vulnerable.”<sup>9</sup>

The insight that vulnerability is not binary is critical. Several insights follow. The first is that no one is entirely invulnerable at all times and in all contexts. We are all vulnerable in degrees and according to circumstance. This is especially clear in the consumer context as I describe below.

Some theorists—notably Martha Fineman—would leverage our shared human condition of vulnerability to supplant discrimination as a way to organize equality discourse and redress.<sup>10</sup> The responsibility of the state becomes the recognition and redress of vulnerability as it arises in society according to social, physical, environmental, or other forces. At the same time, although everyone is vulnerable to a degree, some individuals and groups within society are more vulnerable than others. A person of color may lack privileges as basic as the benefit of doubt, which in turn renders him or her systematically vulnerable to abuses of government power.<sup>11</sup> Scholars have critiqued vulnerability theory on this basis.<sup>12</sup>

The second insight is that vulnerability is not entirely a product of happenstance. The circumstances that correlate to vulnerability can be controlled or engineered, and, thus, so can vulnerability itself. Vulnerability is not, or at least not exclusively, a naturally occurring phenomenon. A person, group, or society could *exploit* the vulnerability it happens to come across in the world—as when an unscrupulous caretaker exploits the vulnerability of an elderly charge in an effort to divert her will. But, separate and apart, a person, group, or society could *render* a person more vulnerable by exposing that person to particular circumstances, actions, or

---

<sup>8</sup> For example, the Supreme Court for a time recognized the need for special protections from attorney solicitation while a person was recovering from injuries. See *Ohralik v. Ohio State Bar Ass’n*, 436 U.S. 447, 464-65 (1978).

<sup>9</sup> See Florencia Luna, *Elucidating the Concept of Vulnerability: Layers Not Labels*, *Int’l J. Feminist Approaches to Bioethics*, Spring 2009, at 121, 129 (my emphasis).

<sup>10</sup> See Martha Albertson Fineman, *Beyond Identities: The Limits of an Antidiscrimination*, 92 *B.U. L. Rev.* 1713 (2012); Martha Albertson Fineman, *The Vulnerable Subject and the Responsive State*, 60 *Emory L.J.* 251 (2010).

<sup>11</sup> Cf. Cheryl I. Harris, *Whiteness as Property*, 106 *Harv. L. Rev.* 1707 (1993).

<sup>12</sup> E.g., Frank Rudy Cooper, *Always Already Suspect: Revising Vulnerability Theory*, 93 *N.C. L. Rev.* 1339, 1342 n.9 (2015) (critiquing vulnerability theory for its refusal to acknowledge the role of identity); Nancy E. Dowd, *Unfinished Equality: The Case of Black Boys*, 2 *Ind. J.L. & Soc. Equality* (2013).

information. Tal Zarsky furnishes the example of a consumer who receives a complementary pack of cigarettes with his groceries when the store figures out he is contemplating quitting.<sup>13</sup> And again, this choice to exploit or render may in turn fall disproportionately across society on the basis of demographic or other factors.

The remainder of the essay explores these two insights in greater depth.

### **Privacy as a shield**

Lex Luthor, the great enemy of Superman, was originally depicted as a mad scientist with access to futuristic weaponry. By the time of Gene Hackman's famous portrayal in the 1978 film *Superman*, Luther is just a very clever businessperson.<sup>14</sup> He is nevertheless able to capture and almost kill Superman, who escapes only when Luthor's girlfriend frees him in order to save her family. How does an ordinary person like Luthor nearly defeat the Man of Steel?

Knowledge about a person confers power over that person. It makes the person vulnerable. A straightforward enough example is physical vulnerability. If you know that a person is allergic to peanuts (or kryptonite) you could use that information to make them very sick. Absent this knowledge you have no such power.

Whether knowledge creates vulnerability can depend on context. Generally there is no threat to person A if person B knows her location. Unless, of course, person B is the perpetrator of intimate partner violence against person A. That is why mapping services like Google Maps that make the world more discoverable work with domestic violence groups to help ensure no information about them appears in the database.<sup>15</sup>

A second, related vulnerability is the prospect of blackmail. The FBI famously sought to blackmail Dr. Martin Luther King, Jr. by threatening to reveal alleged extramarital affairs evidenced through (illegal) wiretaps.<sup>16</sup> But one need not rely on this extreme, historic example regarding a highly visible individual. Paul Ohm speculates that nearly everyone has a fact about them that could be ruinous were it widely shared—what Ohm calls a database of ruin.<sup>17</sup> If so, this opens each of us open to the prospect of being made vulnerable through its discovery.

---

<sup>13</sup> Tal Z. Zarsky, *Mine Your Own Business! Making the Case for the Implications of Data Mining of Personal Information in the Forum of Public Opinion*, 4 *Yale J.L. & Tech.* 5 (2002).

<sup>14</sup> *Superman: The Movie* (Warner Bros. 1978).

<sup>15</sup> Ryan Singel, *Google Map Makers Reaches Out To Anti-Domestic Violence Community*, *Wired* (May 19, 2007).

<sup>16</sup> For a discussion, see Neil M. Richards, *The Dangers of Surveillance*, 126 *Harv. L. Rev.* 1934, 1953-55 (2013).

<sup>17</sup> Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 *UCLA L. Rev.* 1701, 1748 (2010).

A third example involves persuasion. In his chilling book *Lexicon*, Max Barry dreams up a world in which Poets learn to overcome a subject's will through a particular string of words that break down the mind's resistance.<sup>18</sup> Each person's string is different in accordance to their segment, i.e., their particular psychological category. A skilled Poet need only determine a person's segment and is able to take them over completely. (Poets themselves take great care not to reveal anything about themselves—for instance, by selecting office décor at random.)

*Lexicon* is science fiction.<sup>19</sup> But the notion that understanding a person can lead to control over them is not. In previous work around consumer privacy, I have explored a different sense in which information about a person renders them vulnerable. We know from the study of behavioral economics that consumers do not always act rationally in their self-interest. Indeed, people often behave *irrationally* in largely predictable ways due to so-called cognitive biases. Presumably, not everyone has the same cognitive biases, or to the same degrees. Thus, a firm (company) with access to how a particular consumer deviates from rational decision making has both the incentive and the means to extract rent from that consumer by manipulating the circumstances of their interaction—what I call digital market manipulation after the work of Jon Hanson and Douglas Kysar.<sup>20</sup>

Privacy acts as a shield in these and other contexts by placing barriers in the way of discovering or rendering vulnerability. Precisely how Lex Luther discovered Superman's susceptibility to kryptonite is unclear. But presumably Superman could have used better information security. Location privacy lends greater physical security for a significant portion of the population. Information privacy keeps our databases of ruin out of the hands of those who would exploit us. And a stronger consumer privacy regime would make it more difficult for firms and others to discover and hence exploit our cognitive biases.<sup>21</sup>

At a basic level, then, one function of privacy is to minimize the exploitation and rendering of vulnerability by hiding the vulnerability itself (e.g., location or peanut

---

<sup>18</sup> Max Barry, *Lexicon: A Novel* (2013). Evan Selinger observed, and I agree, that Barry's reference to "Poets" is likely an allusion to Plato's warning in the Republic that poets are dangerous to the ideal city because of their capacity to stir the emotions of citizens. Plato, G.M.A. Grube & C.D.C. Reede, *Republic*, Book X (1992).

<sup>19</sup> Mostly. There is a relatively new branch of study that examines how better to persuade consumers and others by determining their psychological make up. It is called persuasion profiling. See, e.g., Maurits Kaptein & Dean Eckles, *Heterogeneity in the Effects of Online Persuasion*, 26 *J. Interactive Marketing* 176 (2012).

<sup>20</sup> Ryan Calo, *Digital Market Manipulation*, 82 *Geo. Wash. L. Rev.* 995 (2014), citing Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation*, 74 *N.Y.U. L. Rev.* 630 (1999).

<sup>21</sup> Or we may wind up turning this information over voluntarily. See Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of Full Disclosure*, 105 *Nw. U. L. Rev.* 1153 (2015).

allergy) or by protecting the information that, if known, would render us vulnerable in the moment.

As noted above, vulnerability is not distributed evenly across society. On the one hand, certain consumers—those with more resources, for instance, or with cultural influence—might find themselves more often targeted by certain advertisers. On the other hand, factors such as race or socioeconomic status can render individuals or groups vulnerable in more contexts. There is substantial evidence that the more vulnerable a person is in society, the greater the societal expectation that they shed privacy. Work by Khiara Bridges, for examples, illustrates the extent to which “the poor barter their privacy rights in exchange for government assistance.”<sup>22</sup> Whereas an insured mother expect privacy around her prenatal care, a mother requiring public assistance must answer barrage of highly person questions.<sup>23</sup>

Bridges’ observation arises in the context public health services; other examples include welfare, employment, and criminal justice.<sup>24</sup> Common across these contexts and others is a similar compounding effect. The more information you have about a person or group, the greater the potential to take advantage of them. But the less advantages a person or group already enjoys, the lesser their ability to resist expectations and requirements of turning over information in exchange for support. The result is a vicious cycle—which bears great exploration and may militate in favor of stronger privacy protections for the chronically vulnerable.

### **Privacy as a sword**

Thus far the discussion has suggested that greater vulnerability results from an absence of privacy or that privacy’s protections are denied to the vulnerable. But privacy bears an even darker relation to vulnerability. Privacy can hide the creation and exploitation of vulnerability itself, both literally and figuratively.

Just above I discuss how firms might use what they know about consumers to take advantage of them. But firms invoke privacy even as they compromise it. Many companies cling to trade secret protection and other laws to avoid having to describe the processes by which they study and sort consumers at granular level.<sup>25</sup>

---

<sup>22</sup> Khiara M. Bridges, *Privacy Rights and Public Families*, 34 *Harv. J.L. & Gender* 113 (2011). Michele Goodwin’s contribution to this very symposium also highlights the degree to which debt collection in the health context falls disproportionately on the already disadvantaged. Michele Goodwin, *Hospital Snitches: Debt Collection and Corporate Responsibility*. Thank you to conference participant Danielle Keats Citron for pointing me toward Bridges’ research.

<sup>23</sup> See also Ryan Calo, *Privacy and Markets: A Love Story*, 91 *Notre Dame L. Rev.* 649, 679-81 (2015) (arguing that the market mechanism is at least theoretically more privacy friendly than social distribution).

<sup>24</sup> See Michele Estrin Gilman, *The Class Differential in Privacy Law*, 77 *Brook. L. Rev.* 1389 (2012).

<sup>25</sup> Nor is this practice limited to the private sector. See David S. Levine, *Secrecy and Unaccountability: Trade Secrets in our Public Infrastructure*, 59 *Fla. L. Rev.* 135 (2007).

The digital environments a company engineers—its websites and apps—are not transparent to the user and attempts to reverse engineer this code can be met with a lawsuit.<sup>26</sup>

Terms of service appear to be written purposefully to maximize allowances while minimizing technical description. Thus a company might say that it uses consumer information to provide services, including advertising, without conveying any real information on how this occurs.<sup>27</sup> When companies talk about how a service works, regulators without technical expertise must largely take the firm's word. Recent developments have seen improvements, however, both in the degree of corporate transparency and in the technical capacity of regulatory bodies to scrutinize information systems.<sup>28</sup>

The idea that privacy can be invoked as a shield against accountability for vulnerability rendering and exploitation is neither limited to the technology context nor particularly novel. Feminist legal scholars such as Catherine MacKinnon and Reva Siegel have long argued that privacy exists in large measure to protect the spaces and practices by which women are subjugated.<sup>29</sup> MacKinnon argues that privacy is foremost a right of the powerful to be left alone by the state—a freedom the powerful use largely to oppress the vulnerable.<sup>30</sup> This idea, while contested, is clearly true to a degree: great harm happens behind closed doors.<sup>31</sup>

Privacy is also deployed against the vulnerable at the level of rhetoric. Recently we have seen the notion of privacy invoked rather explicitly to keep a vulnerable population vulnerable. Specifically, several states passed laws that prohibit local municipalities from establishing mixed gender bathrooms or permitting people to

---

<sup>26</sup> The most common arguments involve the anti-circumvention provision of the Digital Millennium Copyright Act and, as in the recent *Facebook v. Vachani* decision in the Ninth Circuit, the Computer Fraud and Abuse Act prohibition on unauthorized access to a protected computer. *Facebook v. Vachani*, No. 12-17102 (9<sup>th</sup> Cir. Jul. 12, 2016).

<sup>27</sup> Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 *Notre Dame L. Rev.* 1027, 1062 (2012).

<sup>28</sup> The Federal Trade Commission in particular has actively recruited technologists to help the Commission identify and redress digital harms.

<sup>29</sup> Catherine A. MacKinnon, *Privacy v. Equality: Beyond Roe v. Wade*, in *Applications of Feminist Legal Theory to Women's Lives: Sex, Violence, Work, and Reproduction* (D. Kelley Weisberg, ed., 1996); Reva B. Siegel, "The Rule of Love": Wife Beating as Prerogative and Privacy, 105 *Yale L.J.* 2117 (1996).

<sup>30</sup> MacKinnon, *supra*.

<sup>31</sup> This is sometimes portrayed as a "radical" argument and, to the extent MacKinnon would conceive of all of privacy as a mask for subjugation, it likely is. But clearly there is truth to the idea that vulnerability rendering and exploitation occurs behind privacy's doors. For an argument that privacy and the subjugation of women are not inexorably linked, see Annabelle Lever, *Must Privacy and Sexual Equality Conflict? A Philosophical Examination and Some Legal Evidence*, *Social Research* 67:4 1137-71 (2000).

use the bathroom consistent with their gender identity. One such law—called the Public Facilities Privacy and Security Act—requires people to use the bathroom corresponding to the gender on their birth certificate.<sup>33</sup>

These laws reflect back the moral outrage experienced by members of these communities against transgender people. They are about withdrawing protection. But privacy is the way these laws have been formally and publicly justified. The idea is that it violates a person's privacy to be in the same bathroom as someone they conceive of the opposite gender, even if that person's own experience of their gender differs, and even in places—like women's bathrooms—that consist entirely of stalls with doors.

Note the dual sense in which this privacy rationale enforces vulnerability. First, the target population is already vulnerable (in the classic legal sense grounded in status or relationship) insofar as individuals' gender identity differs from mainstream expectation.<sup>34</sup> And second, the context of the bathroom is one in which everyone—of any gender identity—experiences vulnerability. That is why the privacy rationale gets so much traction and, at the same time, exactly why the violence to the vulnerable target population is particularly intense.<sup>35</sup>

Finally, privacy can obscure the very concept of vulnerability. I have argued that there is a cost to attaching the label "privacy" to context where the real harm at issue may involve vulnerability.<sup>36</sup> Thus, for example, *Griswold v. Connecticut* famously invokes privacy (between a doctor and his patient) to place limits on the state's ability to control contraceptive use.<sup>37</sup> *Stanley v. Georgia* invokes privacy to push back against government censorship of obscenity.<sup>38</sup> And *Lawrence v. Texas* invokes privacy again to explain why the state cannot prohibit sodomy.<sup>39</sup>

Arguably the values at issue in these and other cases deal less in privacy than in the freedoms citizens should hold to deviate from societal or community expectation. Further, we might wonder whether characterizing the issue as privacy cabins the import of these decisions to private spaces. The statement "women should be able to make decisions about their own bodies" or "men should be able to have sex with

---

<sup>33</sup> Public Facilities Privacy & Security Act, House Bill 2 (2016).

<sup>34</sup> Alternatively, the individual may be in the presumably vulnerable position of exploring the exact contours of gender identity.

<sup>35</sup> Note the parallel to vulnerability theory and its critiques by identity theorists. See *supra*.

<sup>36</sup> Ryan Calo, *The Boundaries of Privacy Harm*, 86 *Ind. L. J.* 1131 (2011).

<sup>37</sup> 381 U.S. 479 (1965).

<sup>38</sup> 394 U.S. 557 (1969).

<sup>39</sup> 539 U.S. 558 (2003).

other men” differs qualitatively from the claim that doctors’ offices or bedrooms are private spaces in which the state should not operate.<sup>40</sup>

### **Privacy as affordance**

To summarize the argument so far: the law tends to think of vulnerability as a status held by a person or group or else as a relationship between people or institutions. As the legal literature increasingly recognizes, vulnerability is best understood as layer of personhood—a state that exists more often and to greater degrees in certain people and contexts, perhaps, but exists in everyone sometimes. Moreover, vulnerability is not a naturally occurring phenomenon; it is constructed. Personal information, and therefore privacy, plays a crucial role in both rendering and exploiting vulnerability.

Privacy intersects vulnerability in a variety of complex ways. For example, people or groups without privacy are vulnerable and people who are vulnerable may have fewer opportunities to keep information close. Privacy can help interrupt information asymmetries that permit companies to discover and exploit the ways consumers appear to be vulnerable. At the same time, privacy facilitates vulnerability rendering and exploitation by literally hiding abusive practice, rhetorically as a weapon to justify oppression of the vulnerable, and by figuratively obscuring the real value at issue in a vulnerable context.

A final question might be: given this complex, sometimes contradictory relationship between privacy and vulnerability, how should privacy scholarship approach it? This is not a question I can answer for everyone. The dawning realization that privacy is ultimately about power in myriad forms and ways has led me, personally, to seek a new framework of analysis.<sup>41</sup> Such a framework should recognize the role privacy plays in compromising and protecting privacy for individuals, groups, and institutions. It should be capable of bridging the various senses of privacy as well as the many contexts—private and public, digital and physical—in which privacy arises. And, crucially, it should account for how the very experience and perception of privacy as a sword or a shield varies across the population.

The framework I find most helpful is that of affordance theory. Affordance theory originates in perceptual psychology with the work of James Gibson.<sup>42</sup> Gibson notes

---

<sup>40</sup> A possible counterargument says that privacy acts a bridge to greater tolerance of the underlying conduct. Thus, start by saying that men can have sex in their own bedrooms without state intervention only to later invoke this precedent to strike down a ban on gay marriage. This process may be more comfortable; the question is whether it is necessary. Real people suffered in the years between Lawrence and Obergefell v. Hodges.

<sup>41</sup> The realization has also led others to adopt new methods or justify existing methods in new ways. E.g., Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (2012); Neil M. Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (2014).

<sup>42</sup> See, e.g., James J. Gibson, *The Theory of Affordances*, in Robert Shaw and John Bransford, eds, *Perceiving, Acting, and Knowing: Toward an Ecological Psychology* (1977).

that living creatures, including humans, share the same environment. However, they perceive it differently in accordance to their own “affordances,” i.e., their capabilities and limitations. Thus, a bird perceives a cliff as irrelevant whereas a person perceives it as dangerous. A tree affords hiding to a squirrel but not to a bear. Gibson invokes the concept of affordances to bridge the divide between the physical properties of the world (e.g., stairs and air currents) and the relational properties they afford to particular organisms (e.g., climbing and flight).

Of particular interest to law and the social sciences is the notion, mentioned by Gibson in passing, that people represent affordances to one another. “The richest and most elaborate affordances of the environment,” writes Gibson, “are provide by other animals and, for us, other people.”<sup>43</sup> Many factors—social, physical, technical, cultural—mediate these affordances. I want to focus here on two. The first is the role of *information*. A person is only an affordance if you are able to perceive them as such. Thus, for instance, you may require the assistance of law enforcement and not realize that the plainclothes person a few feet away is a police officer. (Gibson calls these unidentified features of the environment “hidden” affordances.<sup>44</sup>) The second is the role of *law*. A trespasser might think your house affords her shelter, a cannibal that your body affords him nutrition. But property and criminal law say otherwise.<sup>45</sup>

Privacy, too, can be conceptualized as an affordance. Privacy furnishes the capacity to withdraw from the world or to hide information about oneself. As with other features of an environment, what privacy affordances exist varies by personal capacity. A cupboard may afford physical concealment to a child but not an adult. A famous person cannot rely on the anonymity of the crowd. The poor, being reliant upon government and other services, realistically cannot “afford” withdrawal or obscurity—which is why some talk of privacy as a luxury good.<sup>46</sup> People of color may draw greater scrutiny by the surveillance state and hence have both a greater need for and lesser chance to privacy’s affordances.<sup>47</sup>

Privacy as affordance accommodates the complex role of privacy as both a shield and a sword for vulnerability. Privacy can withdraw information from others about our susceptibilities and help protect against externally imposed conditions that trigger vulnerability. Privacy thus empowers the weak by placing limits on the strong.<sup>49</sup> At the same time, privacy withdraws from public scrutiny—or, in some

---

<sup>43</sup> Id.

<sup>44</sup> Id.

<sup>45</sup> Law creates, as a minimum, a counter-affordance.

<sup>46</sup> E.g., Julia Angwin, Has Privacy Become a Luxury Good?, N.Y. Times, Mar. 3, 2014.

<sup>47</sup> For a recent and excellent discussion of the relationship between surveillance and race, see the proceedings of The Color of Surveillance: Government Monitoring of the African American Community, available online at [colorofsurveillance.org](http://colorofsurveillance.org).

<sup>49</sup> Cf. Samuel Bray, Power Rules, 110 Colum. L. Rev. 1172 (2010).

cases, purports to justify—the manufacture and abuse of vulnerability. Privacy thus empowers the strong by withdrawing abuses from scrutiny.

Gibson's theory of affordances could be usefully applied to the study and development of privacy and privacy law. Elsewhere I argue that reference to affordance theory helps interrogate whether American surveillance law and policy has reached the proper equilibrium between privacy and national security.<sup>50</sup> If the law affords citizens the means by which to resist and reform surveillance, but citizens choose not to do so, a better case can be made that the state is adhering to a social contract that permits a degree of surveillance in the interest of national security. But in practice Americans do not have such affordances, which in turn calls the legitimacy of the surveillance state into doubt.

The most pressing set of problems in consumer privacy—the subject of this anthology—are at their core similar: in the current environment, only firms possess meaningful affordances. Companies can collect data without asking, condition interactions on the provision of other data, and in general underrepresent the utility of data to the firm and the corresponding danger to the consumer. Moreover, companies—having access to consumer behavior and the ability to “code” the technical and legal environment in which transactions take place—are able to shape the affordances of the consumer to a far greater degree than consumers, individually or collectively, can shape those of the firm.

Consumers appear to have choices that would permit them to protect themselves and police the market; however, as a range of scholars have argued over the past decade, those choices are often illusory. Consumers are vulnerable to firms but not the reverse. This asymmetry of information and power is ultimately unhealthy and unsustainable.

The role of the policymaker, broadly understood, may be to help restore balance in the set of respective affordances of consumers and firms. But the argument I wish to advance here has to do with the approach of privacy scholarship itself. I believe the notion of technical, economic, and legal affordances can help structure and unify the study of consumer privacy. We can ask, within this framework, questions around whether a consumer perceives a set of privacy affordances—including design choices (e.g., encryption), market choices, and legal resources. We can ask whether those perceptions are true, i.e., whether the affordance is actual or “false” or what effect the perception has on consumer behavior. And we can examine whether the affordances vary according to demographics or other factors in ways we consider problematic. A complete account of privacy as affordance is beyond the scope of this essay, but I see it as a promising means by which to explore not only the intersection of vulnerability and privacy but privacy in general.

---

<sup>50</sup> Ryan Calo, *Can Americans Resist Surveillance?*, 83 U. Chi. L. Rev. 23 (2016).

## **Conclusion**

Privacy is a concept that seems to lend itself to an instrumentalist understanding.<sup>51</sup> Privacy exists toward some, usually positive end in society. When it comes to the intersection between privacy and vulnerability, however, the picture is rather complex. Privacy can be both a shield against vulnerability and a sword in its service. What is needed to capture this complex interaction is a theoretical lens rooted in the physical and social environment as it exists, but also sensitive to the differing ways people perceive and experience that environment. Although full throated defense of privacy as affordance is beyond the scope of this essay, James Gibson's theory is an interesting candidate to capture this complexity.

---

<sup>51</sup> See Ruth Gavison, Privacy and the limits of the Law, 89 Yale L.J. 421 (1980).