Can Americans Resist Surveillance?

Ryan Calo†

This Essay analyzes the ability of everyday Americans to resist and alter the conditions of government surveillance. Americans appear to have several avenues of resistance or reform. We can vote for privacy-friendly politicians, challenge surveillance in court, adopt encryption or other technologies, and put market pressure on companies not to cooperate with law enforcement.

In practice, however, many of these avenues are limited. Reform-minded officials lack the capacity for real oversight. Litigants lack standing to invoke the Constitution in court. Encryption is not usable and can turn citizens into targets. Citizens can extract promises from companies to push back against government surveillance on their behalf but have no recourse if these promises are not enforced.

By way of method, this Essay adopts Professor James Gibson's influential theory of affordances. Originating in psychology, and famous everywhere but in law, affordance theory has evolved into a general method of inquiry with its own useful vocabulary and commitments. This Essay leverages these concepts to lend structure to an otherwise-haphazard inquiry into the capabilities of citizens to perceive and affect surveillance. This Essay contributes to affordance theory by insisting that law itself represents an important affordance.

INTRODUCTION

The question in the title is far from straightforward. The majority of Americans who are concerned about government surveillance (52 percent)[1] or who believe that there are inadequate limits on surveillance in place (65 percent)[2] appear to have several avenues for resistance or reform.[3] Americans could elect more representatives who care about privacy. They could challenge surveillance practices under the Constitution. They could

† Assistant Professor of Law, University of Washington School of Law and (by courtesy) University of Washington Information School; Affiliate Scholar, Stanford Law School Center for Internet and Society and Yale Law School Information Society Project. Thank you to *The University of Chicago Law Review* and to participants in its Symposium, and especially to Aziz Huq, Jon Michaels, David Pozen, and Cass Sunstein. Thanks also to the University of Washington Gallagher Law Library for research assistance.

1 Lee Rainie and Mary Madden, *Americans' Privacy Strategies Post-Snowden* (Pew Research Center, Mar 16, 2015), archived at http://perma.cc/SL3E-VSDC.

2 Mary Madden and Lee Rainie, *Americans' Attitudes about Privacy, Security and Surveillance* (Pew Research Center, May 20, 2015), archived at http://perma.cc/CT3X-6N8L.

3 See Rainie and Madden, *Americans' Privacy Strategies* (cited in note 1).

take technological steps to protect their privacy or pressure the companies that hold their data to do so on their behalf.

Yet the various capabilities of Americans to resist surveillance—their antisurveillance "affordances"—turn out to be limited in complex and subtle ways. Elected officials lack the access and expertise that are necessary to conduct meaningful oversight of the intelligence community.[4] Doctrines such as standing have limited the ability of litigants to seek redress for surveillance under the First and Fourth Amendments.[5] And while techniques like encryption and anonymization are capable of checking surveillance in theory, in practice they are not very usable by the people who need them most.[6]

This Essay assesses the capacity of Americans to resist and alter the conditions of government surveillance through politics, law, technology, and markets. Despite some affinities, this analysis breaks from the New Chicago School that has so influenced cyberlaw by popularizing the idea that software itself can act with the force of law in a virtual environment like the Internet.[7] The New Chicago School expands the analytic framework by recognizing "code" and other modalities of regulation beyond law.[8] But the approach is constraining as well: the New Chicago School is centrally concerned with the ability of governments or powerful firms to regulate human behavior rather than the capacity of individuals to negotiate such regulation.[9] The picture is of law and technology as wrestling giants, threatening the citizens underfoot.

This Essay takes a markedly different approach, offering a structured means by which to explore the political, legal, technological, and market-based abilities of Americans on the ground to

---

4 See text accompanying notes 51–52.

5 See text accompanying notes 55–65.

6 See text accompanying notes 75–81.

7 See Lawrence Lessig, *Code: And Other Laws of Cyberspace* 6 (Basic Books 1999) ("In cyberspace we must understand how code regulates. . . . *Code is law*.").

8 See Lawrence Lessig, *The New Chicago School*, 27 J Legal Stud 661, 662–70 (1998) (outlining the "four types of constraint[s]" that regulate behavior: law, social norms, markets, and architecture).

9 See Mark Tushnet, *"Everything Old Is New Again": Early Reflections on the "New Chicago School"*, 1998 Wis L Rev 579, 586–90 (discussing the problems and oversights that result from the New Chicago School's "totalitarian" emphasis on norms). See also Lessig, 27 J Legal Stud at 667–70 (cited in note 8) (discussing some ways in which the modalities of regulation could be used to regulate various behaviors but not addressing the individual's ability to negotiate).

achieve the surveillance conditions that many apparently desire.[10] It selects as a departure point not the New Chicago School, with its emphasis on the capacities of institutions, but the work of psychologist Professor James Gibson, with its emphasis on the capacities of individual organisms to understand and act on the world.

Famous everywhere but law,[11] Gibson introduced the concept of affordances in an effort to structure the study of perception.[12] A key insight of affordance theory is that the same environment or artifact holds different possibilities and dangers for different organisms.[13] A hiding place that affords concealment and secrecy to a child may not afford the same to an adult. The theory of affordances is objective in the sense that features of the environment either do or do not exist, but it is subjective in the sense that the utility or danger to organisms is necessarily relational.

The theory of affordances has influenced disciplines far afield from perceptual psychology.[14] The approach could also be useful to legal scholars interested in what citizens can actually do within a legal system and why. First, as I explore below, affordance theory has evolved into a general method of inquiry with its own useful vocabulary and commitments. This Essay leverages these concepts to lend structure to an otherwise-haphazard inquiry into the capabilities of citizens to perceive and affect surveillance. This Essay meanwhile contributes to affordance theory by insisting that law itself represents an affordance.

Second, the prevalence of everyday affordances can be used as a benchmark by which to test the adequacy of reforms. There is no magical, objectively legitimate amount or degree of surveillance. Nevertheless, we might expect an environment that is rich in affordances to tend toward equilibrium. That is, it seems more plausible to assert that citizens are comfortable with the

---

10 I have selected only a sample of the ways that Americans might resist and reform surveillance, and I then tackle these samples in only limited ways. The scope and purpose of this Essay are modest: the Essay showcases affordance theory as a potentially fruitful means by which to approach complex problems.

11 See text accompanying notes 26–30, 50.

12 James J. Gibson, *The Theory of Affordances*, in Robert Shaw and John Bransford, eds, *Perceiving, Acting, and Knowing: Toward an Ecological Psychology* 67, 67–69 (Lawrence Erlbaum 1977).

13 See id at 79 ("[A]n affordance . . . is a combination of physical properties of the environment that is uniquely suited to a given animal.").

14 Affordance theory has influenced, for example, design, philosophy, web activism, robotics, ecology, and now law. See notes 12, 26–30, 50–51, and accompanying text.

existing balance between privacy and security if they understand and can change that balance but do not do so.[15] As Congress passes new laws and courts revisit old doctrines, affordance theory can help us understand whether these reforms provide real levers of power for citizens.

The remainder of this Essay proceeds as follows. Part I introduces the concept of affordances in further detail, including its reception and development within the technological and other literature. It also briefly introduces the novel concept of a *legal* affordance. Part II applies affordance theory to the titular question whether Americans can resist surveillance. The picture that emerges is complex and warrants further exploration. But we begin to see through affordance theory a sense of why surveillance can persist despite popular distaste and despite the many apparent avenues of resistance. Part III concludes with a discussion of why affordances are perhaps the best benchmark for reform.

I. LAW AND OTHER AFFORDANCES

Professor Gibson, a psychologist, coined the term "affordance" in the 1970s in a bid to integrate and structure the study of perception.[16] Gibson noted that people and other organisms interact with the same environment[17]—but they perceive that environment differently, in part due to each organism's respective abilities and limitations.[18] Thus, a dog and a bird *perceive* the edge of the same cliff as dangerous and irrelevant, respectively. Gibson urged the theory of affordances as an alternative to the cognitive model in which all experiences are subjective and representation takes place entirely "in the head."[19] For Gibson, the world has physical properties (stairs, air currents) as well as relational properties that they afford to the observer

---

15 Professor David Pozen helped me see this implication.

16 See note 12 and accompanying text.

17 Gibson, *The Theory of Affordances* at 70–71 (cited in note 12) (discussing "man's alteration of the natural environment" and proclaiming that "[t]here is only one world . . . and all animals live in it").

18 Id at 79 ("A man . . . measures [ ] features of the environment by the standard of his body.").

19 William W. Gaver, *Technology Affordances*, in Scott P. Robertson, Gary M. Olson, and Judith S. Olson, eds, *Proceedings of the ACM CHI 91 Human Factors in Computing Systems Conference* 79, 79 (ACM 1991).

(climbing, flight). Thus, "an affordance is neither an objective property nor a subjective property; or it is both if you like."[20]

Gibson and others who work within this framework identify a number of important properties of affordances that lend the concept additional structure. Affordances can be *negative* or *positive*, affording either danger or benefit depending on the organism[21]—as with my example of the dog and the bird. Affordances are usually *contingent*, at least to organisms that are capable of altering their environments. For example, a rock face may not afford climbing in the absence of steps or a climbing tool.[22]

Importantly, affordances can be *perceptible* or *hidden*, meaning that there are aspects of the environment that would be perceived as useful or harmful were they observable to the organism.[23] Even if an affordance is perceptible, it can be doubted—Gibson offers the example of a study involving infants who crawl up to a glass surface over a ledge and pat it with their hands but then refuse to believe that the surface affords support.[24] Further, not all perceptible affordances are what they seem: affordances can be *true* or *false*.[25] A false affordance can lead an organism to encounter or fail to avoid harm, as when an organism mistakenly believes that it has an escape route.

Different disciplines have found affordance theory useful for different reasons.[26] Insofar as the theory manages to bridge the objective and the subjective, philosophers invoke the approach in interrogating the relationship between materiality and meaning.[27]

---

20 James J. Gibson, *The Ecological Approach to Visual Perception* 129 (Houghton Mifflin 1979).

21 See id at 137–38.

22 See id at 133–34 ("[W]hat the object affords us is what we normally pay attention to.").

23 See Gibson, *The Theory of Affordances* at 80–82 (cited in note 12) (discussing the "misperceiving" of affordances). Professor William Gaver has noted that organisms can learn to perceive new affordances over time, and he has shown how affordances are often *sequential* (that is, acting on one affordance reveals the presence of another) or *nested* (that is, the affordances work together as a group). Gaver, *Technology Affordances* at 81–82 (cited in note 19).

24 Gibson, *The Ecological Approach to Visual Perception* at 142 (cited in note 20).

25 See Gaver, *Technology Affordances* at 80 (cited in note 19) ("If information suggests a nonexistent affordance, a *false* affordance exists upon which people may mistakenly try to act.").

26 See, for example, Thomas E. Horton, Arpan Chakraborty, and Robert St. Amant, *Affordances for Robots: A Brief Survey*, 3 Avant 70, 73 (2012) (discussing the use of the theory of affordances in the field of artificial technology in order to "develop better agents").

27 See, for example, John T. Sanders, *Merleau-Ponty, Gibson, and the Materiality of Meaning*, 26 Man & World 287, 295 (1993) (applying an affordance analysis to note that

But affordance theory is primarily useful because it suggests a structured means by which to examine the capabilities of a given organism as it interacts with an object or environment. Affordance theory encourages us to ask what an organism situated in the world can really see and do, and what it is about the organism or the environment that makes this so.

Largely for this latter reason, affordance theory has particularly influenced the world of design. Leading design theorist Professor Donald Norman, for instance, discusses the utility of this concept in the design of everyday objects.[28] Proper attention to affordances helps avoid false causality, as when a computer terminal happens to fail just when you touch it.[29] And a well-designed object such as a door should clearly signal its affordances to the user—for example, that the door is to be pushed or pulled.[30]

What of the design of law and legal institutions? As Gibson has recognized, "[t]he richest and most elaborate affordances of the environment are provided by other animals and, for us, other people."[31] We represent to one another innumerable opportunities and risks. Sex, conflict, cooperation, trade, and politics "all depend on the perceiving of what another person or other persons afford, or sometimes on the misperceiving of it."[32] But despite his recognition of its importance, Gibson left the issue there: his germinal work *A Theory of Affordances* does not elaborate on what it means for people to be affordances to one another.

It seems to me that law mediates interpersonal affordances in several ways. First, law helps set the conditions by which we afford. Two or more people engaged in a trade do so against a backdrop of contract law, tort law, and other rules. Variations in the legal status of a person or his environment change his affordances with respect to that environment. A person's home does not afford shelter to others, because of property laws. An unwilling person never affords nutrition to others, even in the most extreme circumstances, in part due to long-standing prohibitions on

---

significance is something "*found* in the world" rather than "*attributed* to otherwise 'neutral' things").

28 Donald A. Norman, *The Design of Everyday Things* 9–12 (Basic Books 2002).

29 Id at 11 (noting that coincidences like the computer-terminal failure lead the user "to believe that [the touching] caused the failure").

30 See id at 87–92.

31 Gibson, *The Ecological Approach to Visual Perception* at 135 (cited in note 20).

32 Id.

cannibalism.[33] The law also permits or denies the prospect of group affordances by, for example, protecting unions or providing for incorporation.

Second, and relatedly, the law itself represents a set of affordances. Individuals or groups can turn to the law for recourse or find themselves at risk because others have done so. Legal affordances have the same basic features that I have already described. You can realize or fail to realize that you have recourse at law. You can think that you have recourse at law but be wrong. And, of particular interest to this Essay, not every person has the same legal affordances, even when a violation of law has clearly occurred. I realize, of course, that the law is famously subject to interpretation.[34] Perhaps law does not exist in an objective state in the way that, for example, a stairway does. But statutes and cases declare law, and we treat certain rights as immutable and real.

Though there is next to no mention of Gibson in the legal literature,[35] we do see echoes of and sympathies to his work. For example, the area of Legal Culture is interested in how social relations predict who will invoke the law and under what circumstances,[36] as is New Legal Realism.[37] Other legal scholarship has

---

[33] See, for example, *Regina v Dudley and Stephens*, 14 QBD 273, 288 (1884) (holding starving sailors criminally liable for killing and eating a nonconsenting passenger).

[34] See, for example, Lon L. Fuller, *Positivism and Fidelity to Law—a Reply to Professor Hart*, 71 Harv L Rev 630, 661–69 (1958) (arguing that judicial interpretation must account for complex and difficult factors and must go beyond a focus on only the fixed meanings of individual words).

[35] The Dutch law-and-technology scholar Professor Mireille Hildebrandt invoked Gibson in her examination of profiling technologies, which for Hildebrandt "seem[ ] to 'afford' a criminal justice system that holds citizens responsible for displaying characteristics that match criminal profiles." Mireille Hildebrandt, *Proactive Forensic Profiling: Proactive Criminalization?*, in R.A. Duff, et al, eds, *The Boundaries of the Criminal Law* 113, 121 (Oxford 2010). Her focus is on technological affordances, however, not legal ones, and she tends to share with the New Chicago School an emphasis on the normative and behavioral implications of technology. See id at 121–22 (discussing "the constitutive and regulative normativity of technologies" and arguing that technologies afford rather than cause new behaviors). Professor Julie E. Cohen has also briefly invoked the concept of affordances to describe how systems place artificial or arbitrary limits on users, which may explain why she cited to Norman instead of Gibson. Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* 195 & n 10, 217–18 (Yale 2012) (expressing concern over "[l]egal rules that prohibit and punish unauthorized access to networked resources" and "the innate tendency . . . to take the configurations of spaces and the affordances of artifacts as givens").

[36] See generally S.S. Silbey, *Legal Culture and Legal Consciousness*, in Neil J. Smelser and Paul B. Baltes, eds, 13 *International Encyclopedia of the Social & Behavioral Sciences* 8623 (Elsevier 2001).

[37] See, for example, Mark C. Suchman and Elizabeth Mertz, *Toward a New Legal Empiricism: Empirical Legal Studies and New Legal Realism*, 6 Ann Rev L & Soc Sci

looked to the capabilities approach, a concept from institutional economics that is associated with Professors Amartya Sen and Martha Nussbaum, which assesses political systems by reference to the freedoms or capacities of their denizens.[38] Capabilities are, in a sense, affordances writ large in that they measure the potential for human flourishing within a society by reference to the physical, emotional, and other goals that members are able to effectively pursue and accomplish.

Even the set of affordances that I investigate below—legal, market, technological, and political—roughly maps onto the four modalities of the New Chicago School—law, markets, architecture, and norms—by which powerful entities can be said to "regulate" individuals and groups. The key difference is that affordance theory starts with the pragmatic conditions that people can perceive and influence rather than with the theoretical methods by which large institutions constrain behavior. In short, this approach is new but not terribly far afield of available methods.

II. SURVEILLANCE: AN AFFORDANCE-BASED APPROACH

This Part analyzes the question in the title—whether Americans really can resist or reform government surveillance—by examining the affordances of everyday citizens and groups. There is not space for a full examination, which would require greater depth and breadth than this Essay can accommodate. Rather, the aim of this Part is to apply the concepts and vocabulary of affordance theory to show that affordances in the surveillance context vary by organism and are not always what they first appear.

I ultimately analyze only a sampling of the affordances of everyday Americans to resist and reform surveillance: voting, litigating, hiding, and buying. I have selected relatively common, paradigmatic examples of asserting influence through politics, law, technology, and markets. Obviously missing are many other means of action and expression, such as art, protest, civil

555, 561 (2010) (noting New Legal Realism's "ground-level up perspective that draws attention to the effect of law on the everyday lives of ordinary people").

[38] For more on the capabilities approach, see Amartya Sen, *Human Rights and Capabilities*, 6 J Hum Dev 151, 153 (2005) (defining a "capability" as "the opportunity to achieve valuable combinations of human functionings—what a person is able to do or be").

disobedience, and education.[39] Such activities, while abundant and disparate, operate through the same basic channels of influence. Civil disobedience works, when it does, because it forces courts or politicians to confront and remedy an injustice. I imagine that an affordance approach, which I propose and briefly showcase here, would also yield insights if applied to art, education, protest, and other examples.

A. Political Affordances

Democracy is set up, in theory, to make politicians affordances for their constituents.[40] Perhaps the most obvious way that citizens of a democracy could influence surveillance policy would be to elect reform-minded leaders. One might think that a concerted-enough effort here could substantially change the way that we balance national security against civil liberties in the United States. And indeed, Congress recently took the occasion of the sunset (by statute)[41] and invalidation (by the United States Court of Appeals for the Second Circuit)[42] of the bulk collection of American phone data by the NSA as an occasion to require more process before the NSA can access these records. Many other collection activities continue apace, however, and few hold their breath for a political sea change.

Will privacy-minded politicians act as citizens expect? One way to think about the disconnect between what many Americans say about their surveillance preferences and their lack of political action is through the lens of public-choice theory.[43] This

---

[39] For an example of work blending these strategies, see *Camouflage from Face Detection* (CV Dazzle), archived at http://perma.cc/34EU-2ZX6.

[40] See Federalist 57 (Madison), in *The Federalist* 384, 385 (Wesleyan 1961) (Jacob E. Cooke, ed) ("[Representatives] will enter into the public service under circumstances which cannot fail to produce a temporary affection at least to their constituents. There is . . . some pledge for grateful and benevolent returns.").

[41] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015 ("USA FREEDOM Act"), Pub L No 114-23, 129 Stat 268.

[42] The NSA claimed authority to engage in bulk data collection under § 215 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), Pub L No 107-56, 115 Stat 272, 287–88, codified as amended at 50 USC §§ 1861–62. Section 215 was invalidated in *American Civil Liberties Union v Clapper*, 785 F3d 787 (2d Cir 2015). See id at 812–13 (holding that the bulk data were not relevant to counterterrorism investigations and therefore that collection was not authorized by statute).

[43] For an early and influential discussion of preferences and public-choice theory, see generally James M. Buchanan and Gordon Tullock, *The Calculus of Consent: Logical Foundations of Constitutional Democracy* (Michigan 1962).

story says that American preferences are diffuse across the population and that they are weakly held. In contrast, the interests of the intelligence community, public and private, are very intense; that community is highly motivated, more homogenous in its values and goals, and close to the levers of power.[44] Under these circumstances, it should hardly surprise us that Americans cannot achieve an ideal balance between security and liberty. In the language of affordances, which again are subjective to the extent that they are relational by organism, we might say that the political process is a perceived but false affordance for citizens while it is a very true affordance for special interests.

Public choice has some explanatory power in privacy law. One of the most careful and extensive examinations of attempts to achieve privacy through the political process comes from Professor Priscilla Regan.[45] She looked at several case studies—including wiretaps and computer databases—in an effort to unpack the various policy dynamics behind federal lawmaking.[46] Regan observed that, in each instance that she examined, vested interests won out over privacy advocacy.[47] She concluded that for meaningful change to occur, we must elevate privacy as a substantive societal value as well as wait patiently for a "policy window" in which to act.[48]

But even if there were broader support for privacy over surveillance, another problem arises regarding the affordances of politicians themselves. As discussed above, design theorist Professor Gaver has introduced the concept of a *nested* affordance, by which he means an affordance that leads to others.[49] Professors Jennifer Earl and Katrina Kimport, both sociologists, have offered the concept of *leveraged* affordances to describe "digitally enabled social change."[50] Their context is technology, but the insight is just as

---

44 For a discussion of the strengths of focused privacy interests, see Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* 174–211 (North Carolina 1995).

45 See generally id.

46 For Regan's discussion of wiretaps, see id at 109–43. For Regan's discussion of computer databases, see id at 69–108.

47 Id at 174, 181–90 (noting that each privacy issue addressed was "on the congressional agenda for years, if not decades, before Congress passed legislation" and weighing the role of interest groups in this delay).

48 Regan, *Legislating Privacy* at 199 (cited in note 44), citing generally John W. Kingdon, *Agendas, Alternatives, and Public Policies* (Little, Brown 1984).

49 See notes 19, 23.

50 Jennifer Earl and Katrina Kimport, *Digitally Enabled Social Change: Activism in the Internet Age* 33 (MIT 2011) ("That a technology such as a computer or the Web *can*

applicable to people. Politicians can be seen as the affordances of the citizenry because they are, in theory, responsive to their constituents. But if they lack affordances of their own in a particular domain, then no degree of responsiveness will create an affordance for the citizenry.

Put another way, politicians are true affordances for citizens to the extent that they have affordances themselves—in other words, to the extent that they are actually in a position to conduct meaningful oversight of the intelligence community. Work in law and political science (and to some extent, common sense) suggests that politicians are not so positioned. With respect to national intelligence, specifically, political scientist Professor Amy Zegart has discussed why congressional oversight of the executive branch remains elusive even in the face of statutory schemes that provide for it.[51] She has pointed in particular to politicians' lack of information about surveillance programs and, more importantly, their lack of expertise to assess the information that they have. As Zegart has put it, "expertise is critical and always in short supply."[52]

B. Legal Affordances

Elected officials are not citizens' only recourse. The United States is a constitutional democracy, founded in a context of skepticism about governmental power and the tyranny of the many. An important purpose of our third branch of government is to render meaningful the guarantees of the Constitution, including those provisions—such as the First Amendment's dictates around speech and assembly or the Fourth Amendment's warrant requirement—that implicate surveillance. The states also have constitutions, some of which directly mention privacy.[53]

---

offer an affordance doesn't really matter unless *people* leverage that affordance. We call this the leveraged affordances approach.").

[51] See generally Amy B. Zegart, *The Domestic Politics of Irrational Intelligence Oversight*, 126 Polit Sci Q 1 (2011).

[52] Id at 9. This claim is in line with what other scholars have observed, including within this Symposium. Additional issues include the lack of visibility (and hence, credit) of good stewardship and extreme risk aversion should terrorist activity actually occur. See, for example, Cass R. Sunstein, *Beyond Cheneyism and Snowdenism*, 83 U Chi L Rev 271, 285 (2016) (discussing the "epistemic difficulty" of quantifying the costs and benefits of national-security safeguards).

[53] See, for example, Cal Const Art I, § 1 (listing the pursuit of privacy as among citizens' "inalienable rights"); Hawaii Const Art I, § 6 ("The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest."); Ill Const Art I, § 6 ("The people shall have the right to be secure . . . against . . .

In theory, then, courts afford individuals and groups a number of ways to challenge surveillance. But while the law sets a baseline for what is permissible and checks the worst abuses, the courts have not historically afforded a meaningful avenue of reform.[54] It is not that surveillance proceeds entirely in the absence of legal limits but rather that the citizen does not possess a significant legal lever to limit surveillance beyond today's baseline levels. Thus, constitutional law can also be a false or misleading affordance in practice.

This is true for a few reasons. One involves issues of harm and standing. Generally speaking, it is not as though any citizen concerned about surveillance can challenge it under the First or Fourth Amendment. Rather, the citizen must have a specific interest in a particular intrusion. In the First Amendment context—that is, when the monitoring of a person or group by the government is extensive enough to implicate free speech—the citizen generally must show that he is in fact being watched and that this monitoring chills his ability to assemble or to express himself.

This turns out to be difficult. Much surveillance occurs in secret, such that litigants cannot show that they are in fact being watched. Courts have even implied that the very act of suing can be evidence that a litigant has not been cowed. Thus, in *Laird v Tatum*,[55] the Supreme Court acknowledged that "constitutional violations may arise from the deterrent, or 'chilling,' effect of governmental regulations that fall short of a direct prohibition against the exercise of First Amendment rights,"[56] but the Court ultimately did not find that the respondents before it were chilled.[57] Indeed, the respondents "cast considerable doubt on whether they themselves [were] in fact suffering from any such chill," in part because the petitioners had the temerity to talk about the government's surveillance in public and challenge it in court.[58]

In the Fourth Amendment context, the citizen must show that his own reasonable privacy interest has been unreasonably

---

invasions of privacy or interceptions of communications by eavesdropping devices or other means.").

54 See text accompanying notes 55–65.

55 408 US 1 (1972).

56 Id at 11.

57 Id at 13–14.

58 Id at 13 n 7 (discussing how counsel for the litigants at bar admitted that they were "not people, obviously, who [were] cowed and chilled").

invaded.[59] Until very recently, "claims for facial relief under the Fourth Amendment [were] unlikely to succeed" unless they sought to cure a defect in a warrant clause.[60] A citizen still cannot sue over the invasion of another's interest, even when the unlawfully obtained evidence is introduced against him in court.[61] The recourse of the third party whose interest was invaded (such as the mother of the defendants in *United States v Salvucci*[62]) is limited to tort, which "[t]he Court has failed to nurture and at times has affirmatively undermined."[63] A court will not exclude evidence obtained in clear contravention of the Fourth Amendment unless it was the defendant's Fourth Amendment right that was violated.

This issue is compounded by the contemporary reality that corporations act as custodians of our digital lives. It is often easier for law enforcement to request your web history from Google or AT&T rather than from you. And, generally speaking, the law treats many categories of information transferred from you to a third party like a corporation as less private and hence less well protected by constitutional criminal procedure.[64] This tendency in the law is known, and sometimes lamented, as the third-party doctrine.[65]

A simpler reason for why courts afford less recourse is that unsympathetic and underresourced defendants make unfortunate champions for the rest of society. The point is controverted, but it seems clear at one level that many of the legal affordances against surveillance are set and tested by a deeply unrepresentative sample of society—people that do not necessarily have the same capabilities or motivations as everyone else. We all

---

59 See *Katz v United States*, 389 US 347, 360–61 (1967) (Harlan concurring).

60 *City of Los Angeles, California v Patel*, 135 S Ct 2443, 2449–50 (2015) (clarifying that facial challenges under the Fourth Amendment are not disfavored).

61 See, for example, *United States v Salvucci*, 448 US 83, 85 (1980) (holding that the defendants lacked standing unless "their own Fourth Amendment rights ha[d] in fact been violated").

62 488 US 83 (1980).

63 Akhil Reed Amar, *Fourth Amendment First Principles*, 107 Harv L Rev 757, 785 (1994).

64 See, for example, *United States v Miller*, 425 US 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.").

65 For a discussion of the third-party doctrine, see Daniel J. Solove, *A Taxonomy of Privacy*, 154 U Pa L Rev 477, 528–29 (2006).

wind up with the affordances of the accused criminal, who is in certain respects our lowest common denominator.[66]

The people who are in court litigating against the government over the fruits of police surveillance have a significant, sometimes life-or-death interest in narrowing the capabilities of law enforcement. So you might think that criminal defendants are particularly well suited to push back against surveillance—but not according to Professor Akhil Amar, who has offered a variety of reasons why the accused criminal is a bad proxy for society as whole and, indeed, "an awkward champion of the Fourth Amendment."[67] The criminal is unsympathetic, for instance, and often litigates bad facts, heedless of what this will do to Fourth Amendment precedent in general.[68] The accused criminal rarely has access to a good lawyer.[69] And so on.

Also skeptical is Professor Shima Baradaran, who points out that courts side with the state over defendants in the overwhelming majority (specifically, four out of five) of Fourth Amendment cases.[70] The problem, according to Baradaran, is that individual defendants do not present courts with relevant statistics or other information to help them balance law enforcement's conduct against societal interests in privacy.[71] Thus, courts engage in "blind balancing" that almost invariably inures against the criminal defendant and, by extension, to the innocent citizens whom the Fourth Amendment also avowedly protects.[72]

There are many more ways in which citizens hoping to achieve reform through the courts are stymied, and there are also notable exceptions. My point is that the many citizens who complain of excessive government surveillance cannot always look to the courts to strike a different balance, despite a long constitutional tradition of limited government. They have legal

---

66 See Amar, 107 Harv L Rev at 796 (cited in note 63) ("The criminal defendant is a kind of private attorney general. But the worst kind."). Of course, in the words of Fyodor Dostoyevski, "[t]he degree of civilization in a society can be judged by entering its prisons." Fred R. Shapiro, ed, *The Yale Book of Quotations* 210 (Yale 2006).

67 Amar, 107 Harv L Rev at 796 (cited in note 63).

68 See id.

69 See id.

70 Shima Baradaran, *Rebalancing the Fourth Amendment*, 102 Georgetown L J 1, 43 (2013).

71 Of course, litigants have been introducing broader sociological data since at least the 1900s. See, for example, *Muller v Oregon*, 208 US 412, 419 (1908) (citing the now-famous "Brandeis Brief"). And some judges may feel free to seek out their own sources, including the Internet. See, for example, *Rowe v Gibson*, 798 F3d 622, 628–30 (7th Cir 2015) (relying on Judge Richard Posner's investigation into the efficacy of Zantac).

72 Baradaran, 102 Georgetown L J at 3 (cited in note 70).

rights on paper, including some very old and important paper like the Constitution. But, as with political affordances, the legal affordances of citizens are somewhat limited by judicial precedent and other forces.

C. Technological Affordances

The previous two sections focus, respectively, on the capacity of individuals to restrain government through legislatures and courts. As Professor Lawrence Lessig's interlocutors remind us, individuals and firms have technological means for resistance as well.[73] For the purposes of this Section, I will use the example of encryption to highlight a promising but ultimately limited means by which people can hide from their government.

Encryption, of course, refers to the process of rendering communications unreadable to anyone but the recipient, thereby interfering with surveillance rather directly. Encryption is a straightforward technological affordance in that it affords hiding. And it affords very good hiding: over-the-counter encryption, so to speak, apparently can thwart sophisticated attempts to access protected content.[74] Encryption is very promising. It is a technological affordance that is available to most and does not necessarily rely on the goodwill of third parties. Encryption is no panacea, however, and it also runs the risk of being a false affordance without proper attention.

There are a number of challenges. For encryption to help most citizens, it has to be usable. It often is not. A few years ago, computer scientist Alma Whitten and electrical engineer Professor Doug Tygar conducted a usability assessment of version five of Pretty Good Privacy (PGP), a leading security program with a "good user interface by general standards."[75] They found, famously in computer-security circles, that what makes for usable software in general does not suffice when it comes to security.[76]

---

[73] See, for example, Tim Wu, *When Code Isn't Law*, 89 Va L Rev 679, 707–09 (2003) (describing how people use software to avoid law); James Grimmelmann, Note, *Regulation by Software*, 114 Yale L J 1719, 1742–43 (2005) (discussing how savvy users can evade software restrictions).

[74] See Adrian Covert, *iOS Encryption Is So Good, Not Even the NSA Can Hack It* (Gizmodo, Aug 13, 2012), archived at http://perma.cc/E4SW-CVZ8 (noting that the newest version of the popular iPhone has very good encryption).

[75] Alma Whitten and J.D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*, in Lorrie Faith Cranor and Simson Garfinkel, eds, *Security and Usability: Designing Secure Systems That People Can Use* 669, 669 (O'Reilly 2005).

[76] See id at 689–90.

Their test subjects made errors and, as a consequence, did not actually hide what they were saying.[77]

A much more recent paper looks at the technological affordances of a particular population for whom secrecy and discretion are of great importance. A journalism professor at Columbia University partnered with computer scientists at the University of Washington to undertake an examination of whether available tools of anonymization and encryption work for investigative journalists.[78] Like Whitten and Tygar, this team found that existing technology was still not usable.[79] Further, available technology tended to "actively interfere with other aspects of the journalistic process" such as the verifiability of sources and source information.[80] This was despite the fact that journalists are commonly identified as the very people who need heightened computer security to accomplish their important work.[81]

If encryption is not usable, or, at any rate, if it is not widely used, then those who do use encryption can wind up as targets; a positive affordance becomes a negative one. There are several reasons why the subjects of government surveillance must still worry even if traffic is encrypted. There is always the possibility that, with enough resources thrown at the problem, some encryption will be broken. There is also the ability to compromise the user's computer to access communications before they are encrypted in the first place. And even assuming that the government can see only the direction and frequency of traffic—that is, so-called metadata—the computer science literature is increasingly clear that the government may still make guesses as to the content.[82]

Among the most promising developments for privacy enthusiasts following the revelations of CIA contractor Edward Snowden have been the decisions of Apple, Google, and other companies to

---

77 See id at 689.

78 See Susan E. McGregor, et al, *Investigating the Computer Security Practices and Needs of Journalists* *399 (USENIX, Aug 2015), archived at http://perma.cc/W555-QML3. USENIX is the premiere academic symposium on computer security.

79 See id at *410.

80 Id at *399.

81 See id at *412.

82 Consider Shahram Mohrehkesh, et al, *Demographic Prediction of Mobile User from Phone Usage* (Mobile Data Challenge), archived at http://perma.cc/Q3ZB-APUC (describing the results of a study that attempted to predict a user's demographic attributes using metadata).

encrypt communications by default.[83] Defaulting to encryption obviates the above problems—something that is already turned on need not be usable, and most people stick with defaults, making encryption widespread.[84] The prospect that citizens can pool affordances as consumers is the subject of the next Section.

D. Group or Market Affordances

Even if citizens struggle to invoke their rights individually, perhaps they can use the market to pressure powerful firms to vindicate those rights in their stead. Contemporary companies hold centrally and in bulk most of the personal details that law enforcement is usually after, and firms have the resources to fight government surveillance of their customers.[85] Indeed, the Snowden revelations and subsequent global reaction to the NSA's spying capabilities have invigorated privacy as a competitive differentiator.[86] Firms are making technological changes (some of which are discussed above) and pushing back against subpoenas with greater force.

Just as governments can leverage the market as a modality of regulation—for example, by increasing taxes on undesirable behavior—so too can citizens pool their affordances through the market to pressure larger, organized firms to press their interests. This could be thought of as an instance of nested or sequential affordances, group affordances, or something similar. By any label, we cannot answer the question whether Americans can resist surveillance without thinking through the affordances and incentives of the large corporations that hold their data.

History is not so promising here. As Professor Jack Balkin, Professor Jon Michaels, and others argue, the best way to characterize the past relationship between governments and corporations

---

[83] Joe Miller, *Google and Apple to Introduce Default Encryption* (BBC, Sept 19, 2014), archived at http://perma.cc/9XG4-DVZT.

[84] Of course, the price of liberty is eternal vigilance. Today, law enforcement is actively reigniting the battle over back doors by arguing that the FBI and others should have access to keys that unlock all encryption when necessary. See Dan Kedmey, *Apple and Google Want Obama to Let Them Encrypt Your Phone* (Time, May 19, 2015), archived at http://perma.cc/M2ZN-K7RY.

[85] See, for example, Covert, *iOS Encryption Is So Good* (cited in note 74).

[86] See Solange Deschatres, *Android vs. iOS: Which Is More Secure?* (Forbes, July 24, 2014), archived at http://perma.cc/6FRD-SHDS ("Some might say there are fewer differentiators now between iOS and Android. But here's a breakdown of the host of security threats they face, and the varying ways in which Apple and Google attempt to mitigate them.").

around surveillance is *synergistic*.[87] Firms use government-mandated data and governments leverage private databases and tools. Both firm and government activities erode societal expectations of privacy.

There is also evidence that corporate resistance is relatively rare in practice. Recent work by Professor Avidan Cover examines whether, as some argue, companies can nevertheless stand in the shoes of individuals and assert privacy claims on individuals' behalf.[88] Cover concludes that corporations seldom push back against the government in practice and that when they do, they are hamstrung by a variety of forces.[89] The company, like the criminal defendant, tends to put its own interest before that of the consumer. The government can make life more or less pleasant for a company, including by conferring immunity from suit should consumers get upset.[90] Cover also takes issue, normatively, with the idea that citizens should have to rely on companies to press their freedoms—especially in light of the role that British companies played in the perceived abuses of colonial America.[91]

To these arguments we might add another: promises in this context are especially cheap. A pledge not to cooperate with the government, made for reasons of consumer trust and competition, is not going to be easy to enforce. The market affords greater privacy only if consumers can select privacy as a preference and believe that the preference will be respected. There is reason to think that this preference will not be respected, given that the same government that is asking for the data will also be enforcing the failure to resist.

---

87 See, for example, Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 Minn L Rev 1, 7–8 (2008) ("Public and private enterprises are thoroughly intertwined."); Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 Cal L Rev 901, 904 (2008) (discussing the executive branch's informal agreements with corporations).

88 Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 Iowa L Rev 1441, 1456 (2015), citing Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich L Rev 561, 595–600 (2009).

89 Cover, 100 Iowa L Rev at 1463–73 (cited in note 88).

90 This occurred when Congress conferred retroactive immunity on Internet service providers (ISPs) that cooperated with the NSA through passage of the FISA Amendments Act of 2008 § 201, Pub L No 110-261, 122 Stat 2436, 2467, codified at 50 USC §§ 1885 to 1885c ("[A] civil action may not lie or be maintained in a Federal or State court against any person for providing assistance to an element of the intelligence community.").

91 Cover, 100 Iowa L Rev at 1487–88 (cited in note 88) (describing the role that the East India Company played in starting the American Revolution, as well as the Framers' views on corporations and monopolies).

Take the respective privacy policies of two companies that store and analyze consumers' genetic information. The company 23andMe, which sells saliva-based genome tests to individual consumers, says in its privacy policy that if it receives a lawful request for genetic information, it will turn that information over to the government: "Under certain circumstances Personal Information may be subject to disclosure pursuant to judicial or other government subpoenas, warrants, or orders, or in coordination with regulatory authorities."[92] A competitor of 23andMe, Navigenics, also acknowledges the prospect that the government may seek to compel disclosure, but unlike 23andMe, it commits to "use reasonable and lawful efforts to limit the scope of any such legally required disclosure."[93]

For the many civilian-consumers who worry about privacy, this would seem to suggest that Navigenics is the better choice for personalized genetics. But what happens if Navigenics decides not to push back as advertised? Generally speaking, if a firm makes a promise to its consumers and violates it, those consumers have recourse—a legal affordance—in the Federal Trade Commission (FTC) or state equivalents.[94] The FTC can bring an enforcement proceeding under its authority to police against deceptive statements.[95] Here, however, the FTC—itself a government enforcement agency—would have to penalize Navigenics for cooperating *with another government enforcement agency*. That even an independent agency like the FTC would do this strikes me as very unlikely, and it therefore tends to hollow out this particular kind of market promise.

Nevertheless, it is hard not to see the potential here. Against a background of corporate and other law, and given access to enormous resources, large firms are well positioned to push back against government surveillance if they are properly motivated. That motivation appears to be mounting in the form of domestic and, to a large degree, international pressures on American firms to put citizen-consumer privacy first.

---

92 *Privacy Highlights* (23andMe), archived at http://perma.cc/K9EQ-FZ3R.

93 *Privacy Policy* (Navigenics), archived at http://perma.cc/8AJT-X6C6.

94 See 15 USC §§ 52–54 (authorizing the FTC to pursue penalties or injunctive relief for false advertising, or "unfair or deceptive act[s] or practice[s]").

95 15 USC §§ 41–58.

III. AFFORDANCES AS A BENCHMARK

To summarize the argument so far: An affordance refers to an aspect of the environment that holds promise or danger depending on an organism's capacities. Citizens have a number of perceived affordances when it comes to surveillance—political, legal, technological, and other avenues to resist or effectuate change. But upon inspection, many of these affordances turn out to be false or compromised. Citizens can vote officials who care about privacy into office, but those officials lack the capacity for real oversight. Citizens have technological means by which to resist surveillance, but the technologies lack usability and can turn citizens into targets. Citizens can extract promises from firms to push back against surveillance on their behalf, but they have no recourse if these promises are not enforced.

This is a bleak picture, but there are bright spots as well. Congress enacted modest reforms to NSA surveillance in 2015, and companies have shown an interest in pushing back against demands for consumer data.[96] Recent case law is particularly promising. In a series of Fourth Amendment decisions, the Supreme Court has shown a willingness to interpret the Constitution more favorably, if not more broadly.[97] In the 2015 term, the Court repudiated its prior holding that Fourth Amendment cases were too fact bound to accommodate facial challenges, allowing a hotel owner to challenge a statute that gave the police access to his visitor logs.[98] Another recent decision recognized the intimacy and extent of the data that we keep on our personal devices and clarified that officers cannot search a smartphone merely incident to arrest and without a warrant,[99] which some commentators believe paves the way toward a reexamination of the third-party doctrine.[100]

---

96 Among other things, the USA FREEDOM Act requires ISPs instead of the NSA to store telephone records and makes the Foreign Intelligence Surveillance Court, the court that grants the NSA approval for its activities, more adversarial. See USA FREEDOM Act § 501, 129 Stat at 282–83, codified in various sections of Titles 12, 15, and 18; USA FREEDOM Act § 402, 129 Stat at 281–82, codified at 50 USC §§ 1871–74.

97 Various majority opinions have, in a sense, narrowed the case law in places by tying it closely to the common-law tort of trespass. See, for example, *Florida v Jardines*, 133 S Ct 1409, 1415–17 (2013) (holding that bringing a drug-sniffing dog onto private property requires probable cause); *United States v Jones*, 132 S Ct 945, 949 (2012) (holding that affixing a GPS to a car requires probable cause).

98 See *City of Los Angeles, California v Patel*, 135 S Ct 2443, 2449–51 (2015).

99 See *Riley v California*, 134 S Ct 2473, 2484–88 (2014).

100 See, for example, Ryan Watzel, Riley*'s Implications for Fourth Amendment Protection in the Cloud*, 124 Yale L J F 73, 73–74 (2014) ("[W]hile failing to explicitly afford

We can say, perhaps, that the picture is improving. But we have no real means of describing when the picture has improved *enough*. We lack a benchmark for surveillance reform. Presumably the tolerable—let alone optimal—degree of government surveillance of citizens is not zero, or any specific number. We cannot refer to an ideal amount of money spent on surveillance or point to a particular year that was just fine for privacy. Ask citizens what the right balance is between privacy and security and you are likely to get different answers.

In other words, we cannot say what equilibrium looks like by describing surveillance activity or policy. But we may be able to say more about what equilibrium looks like as a condition. It is here that I see additional utility in the concept of affordances. We can and should evaluate reforms to political institutions, laws, technology, and markets by reference to the effects on the affordances of everyday citizens. If we are ever able to document that people have legitimate and practical means to resist and reform government surveillance, but that they still choose not to do so, then a much stronger case can be made that our society has struck an appropriate balance. As this analysis has shown, we are very far from this utopian place. But perhaps we are a little closer to seeing what it might look like.

CONCLUSION

This Essay poses the important but underexamined question whether Americans have the means by which to resist and reform surveillance. It then introduces the concept of affordances to help structure an answer to that question. In so doing, this Essay makes three contributions. First, it suggests that affordance theory has both something to teach and something to learn from legal theory. Law dictates how people can be affordances to one another, and it is itself a kind of affordance. Second, this Essay examines surveillance affordances of various kinds—political, legal, technological, and market—and in each instance finds limits to otherwise-viable avenues of resistance and reform. Finally, this Essay proposes the proliferation of positive citizen affordances as a benchmark for reform. If Americans can resist surveillance in theory and in practice, then, and only then, their failure to do so gestures toward equilibrium and legitimacy.

Fourth Amendment protection to cloud-based data, *Riley* still provides the best evidence yet that the Court may be ready to reconsider the third-party doctrine.").