Can Americans Resist Surveillance?

Ryan Calo | rcalo@uw.edu
University of Washington School of Law

Legal Studies Research Paper No. 2015-25
U. Chi. L. Rev. (forthcoming)

Electronic copy available at: http://ssrn.com/abstract=2635181

CAN AMERICANS RESIST SURVEILLANCE?

Ryan Calo[*]

INTRODUCTION

The question in the title is far from straightforward. The majority of Americans who are concerned about government surveillance (52%), or believe there are inadequate limits on surveillance in place (65%), appear to have several avenues for resistance or reform.[1] Americans could elect more representatives who care about privacy. They could challenge surveillance practices under the Constitution. They could take technical 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 surveillance "affordances"—turn out to be limited in complex and subtle ways. Elected officials lack the access and expertise necessary to conduct meaningful oversight of the intelligence community.[2] Doctrines such as standing have limited the ability of litigants to seek redress for surveillance under the First and Fourth Amendments.[3] And while techniques like encryption or anonymization are capable of checking surveillance in theory, in practice they are not very usable by the people who need them most.[4]

This essay assesses the capacity of Americans to resist and alter the conditions of government surveillance through politics, law, and technology. Despite some affinities, the analysis breaks from the New Chicago School that has so influenced cyberlaw. The New Chicago School expands our analytic framework by recognizing "code" and other modalities of regulation beyond law.[5] But the approach is constraining as well:[6] the

[*] Assistant Professor, 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, especially Aziz Huq, Jon Michaels, David Pozen, and Cass Sunstein. Thanks also to the UW Gallagher Law Library for research assistance.

[1] Pew Research Center, *Americans' Privacy Strategies Post-Snowden* (Mar. 16, 2015)..

[2] *See infra*.

[3] *See infra*.

[4] *See infra*.

[5] Lawrence Lessig, *The New Chicago School*, 27 J. Legal Stud. 661 (1998).

Electronic copy available at: http://ssrn.com/abstract=2635181

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. The picture is of law and technology as wrestling giants, threating the citizens underfoot.

This essay takes a markedly different approach, offering a structured means by which to explore the political, legal, and technical ability of Americans on the ground to achieve the surveillance conditions many apparently desire.[7] It selects as a departure point not the New Chicago School, with its emphasis on the capacities of institutions, but the work of psychologist James Gibson, with its emphasis on the capacity of individual organisms to understand and act upon the world.

Famous everywhere but law, Gibson introduced the concept of affordances in an effort to structure the study of perception.[8] A key insight of affordance theory is that the same environment or artifact holds different possibilities and dangers for different organisms. A hiding place that affords concealment and secrecy to a child may not afford these things to an adult. The theory of affordances is objective, in the sense that features of the environment exist or do not, but subjective, in the sense that their utility or danger to organisms are necessarily relational.

The theory of affordances has influenced disciplines far afield from perceptual psychology.[9] 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 hopes to leverage these concepts to lend structure to an otherwise haphazard inquiry into the capability of citizens to perceive and affect surveillance. The 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 magic,

---

[6] *Cf.* Mark Tushnet, *Everything Old is New Again: Early Reflections on the New Chicago School*, 1998 Wis. L. Rev. 579 (1998) (discussing what the New Chicago School leaves out).

[7] I have selected only a sample of the ways Americans might resist and reform surveillance, and then only tackled these samples in limited ways. The scope and purpose of this essay is modest: to showcase affordance theory as a potentially fruitful means by which to approach complex problems.

[8] James J. Gibson, *The Theory of Affordances*, in Perceiving, Acting, and Knowing (Robert Shaw and John Bransford, eds. 1977).

[9] Affordance theory has influenced, for instance, design, philosophy, web activism, robotics, ecology, and now law.

Electronic copy available at: http://ssrn.com/abstract=2635181

objectively legitimate amount or degree of surveillance. Nevertheless, we might expect an environment rich in affordances to tend toward equilibrium. That is, it seems more plausible to assert that citizens are comfortable with the existing balance between privacy and security if they understand and can change that balance and do not do so.[10] 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 actual citizens.

The remainder of the essay proceeds as follows. Part I introduces the concept of affordances in further detail, including its reception and development within the technical and other literature. It also briefly introduces a novel concept of *legal* affordance. Part II applies affordance theory to the titular question of 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 it is surveillance can persist despite popular distaste and the many apparent avenues of resistance. A final section concludes with a discussion of why affordances are perhaps the best benchmark for reform.

I. LAW AND OTHER AFFORDANCES

James Gibson, a psychologist, coined the term affordance in the nineteen seventies in a bid to integrate and structure the study of perception. For Gibson, people and other organisms interact with the same environment. But they perceive that environment differently, in part due to each organism's respective abilities and limitations. Thus a dog and a bird *perceive* the edge of the same cliff as dangerous and irrelevant, respectively. Gibson urges the theory of affordances as an alternative to the cognitive model whereby all experience is subjective and representation takes place entirely "in the head."[11] For Gibson, the world has actual physical properties (stairs, air currents) as well as the relational properties they afford to the observer (climbing, flight). Thus, "an affordance is neither an objective nor a subjective property, or it is both if you like."[12]

Gibson and others who work within the framework identify a number of important properties of affordances that lend the concept additional structure. Affordances can be *negative* or *positive*, affording either benefit or danger depending on the organism, as with my example of the dog and

[10] David Pozen helped me see this implication.

[11] William W. Gaver, *Technology Affordances*, Proc. of CHI '91 (Apr. 28 – May 2, 1991), 79-84.

[12] Gibson, *supra* note 8, at 129.

the bird. Affordances are usually *contingent*, at least to organisms capable of altering their environment. A rock face may not afford climbing in the absence of steps or a climbing tool.

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.[13] 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, pat it with their hands, but refuse to believe that the surface affords support.[14] Not all perceptible affordances are what they seem: affordances can be *true* or *false*. A false affordance can lead an organism to encounter or fail to avoid harm, as when an organism mistakenly believes it has an escape route.

Different disciplines have found affordance theory useful for different reasons. In that the theory manages to bridge the objective and the subjective, philosophers invoke the approach in interrogating the relationship between materiality and meaning.[15] But mostly affordance theory is 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 Don Norman, for instance, discusses the utility of the concept in the design of everyday objects.[16] Proper attention to affordances helps avoid false causality, as when a computer terminal happens to fail just when you touch it.[17] And a well-designed object such as a door should clearly signal its affordances to the user, e.g., that it is to be pushed or pulled.[18]

What of the design of law and legal institutions? As Gibson recognizes, "the richest and most elaborate affordances of the environment are provided

---

[13] *Id.* Gaver adds that organisms can learn to perceive new affordances over time, and shows how affordances are often *sequential*, i.e., acting on one affordance reveals the presence of another, or *nested*, i.e., working together as a group. *See* Gaver, *supra* note 11.

[14] Gibson, *supra* note 8, at 142.

[15] *See* John T. Sanders, *Merleau-Ponty, Gibson, and the materiality of meaning*, Man and World 26: 287-302 (1993).

[16] Don Norman, The Design of Everyday Things (2002). This work was originally entitled The Psychology of Everyday Things (1988).

[17] *Id.* at 11.

[18] *Id.* at 91.

by other animals and, for us, other people."[19] We represent to one another innumerate opportunities and risks. Sex, conflict, cooperation, trade, politics "all depend on the perceiving of what another person or other persons afford, or sometimes the misperceiving of it."[20] But despite his recognition of its importance, Gibson leaves 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 that mediates inter-personal affordances in several ways. First, law helps set the conditions by which we afford. Two or more people engaged in trade do so against a backdrop of contract, tort, and other rules. Variations in the legal status of a person or their environment changes their affordances with respect that environment. Someone else's home does not afford shelter because of property laws. One person never affords nutrition to another, even in the most extreme circumstances, in part due to longstanding prohibitions on cannibalism.[21] The law also permits or denies the prospect of group affordances, e.g., by protecting unions or providing for incorporation.

Second, and relatedly, the law itself represents a set of affordances. An individual or group can turn to the law for recourse or find themselves at risk because of others have done so. Legal affordances have the same basic features I've already described. You can realize you have recourse at law, or not. You can think you have recourse at law and be wrong. And, of particular interest to this essay, not every person has the same legal affordances, even where a violation of law has clearly occurred. I realize, of course, that the law is famously subject to interpretation.[22] Perhaps it is not there, objectively, the way a stairway is. But statutes and cases say what they say, and we certainly talk as though certain rights are immutable and real.

Though there is next to no mention of Gibson in the legal literature,[23]

---

[19] Gibson, *supra* note 8, at 135.

[20] *Id.*

[21] R v. Dudley and Stephens, 14 QBD 273 DC (1884).

[22] *See* Lon L. Fuller, Positivism and Fidelity to Law-A Reply to Professor Hart, 71 Harv. L. Rev. 630, 661-69 (1958).

[23] The Dutch law and technology scholar Mireille Hildebrandt invokes James 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," and elsewhere. Mireille Hildebrandt, *Proactive Forensic Profiling: Proactive Criminalization?*, in The Boundaries of Criminal Law 121 (Antony Duff, ed. 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. Julie Cohen also briefly invokes the concept of

we do see echoes and sympathies. For example, the area of Legal Culture is interested in how social relations predict who will invoke the law and under what circumstances[24] as is New Legal Realism.[25] Other legal scholars have looked to the capabilities approach, a concept from institutional economics associated with Amartya Sen and Martha Nussbaum that assesses a political system by reference to the freedoms or capacities of its denizens.[26] Capabilities are, in a sense, affordances writ large. Even the set of affordances I investigate below (legal, market, technical, and political) roughly map to the four modalities of regulation of the New Chicago School—the difference being that affordance theory starts with what people can perceive and affect, rather than how institutions can constrain behavior. In short, the 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 isn't 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 vary by organism and are not always what they first appear.

I look here at only a sampling of the affordances of everyday Americans to resist and reform surveillance: political, legal, technical, and market. I chose these as paradigmatic examples of what Americans can do if they are dissatisfied with the present balance of security and privacy. Obviously missing are the many other means of resistance and reform, such as art, protest, civil disobedience, and education.[27] These and other affordances are

---

affordances to describe how systems place artificial or arbitrary limits on users, which may explain why she cites to the design theorist Don Norman instead of Gibson. Julie E. Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice 195, 217-18 (2012).

[24] *Legal Culture and Legal Consciousness*, in International Encyclopedia of Social and Behavioral Sciences (2001).

[25] *E.g.*, Mark C. Suchman and Elizabeth Mertz, *Toward a New Legal Empiricism: Empirical Legal Studies and New Legal Realism*, Annu. Rev. Law Soc. Sci. 2010. 6:555–79.

[26] For more on the capabilities approach, see Amartya Sen, Human Rights and Capabilities, 6 J. Human Dev. 151, 153 (2005).

[27] These strategies in turn can be blended, as when an artist creates makeup or hairstyles that interfere with facial recognition. You can find Adam Harvey's work at

nuanced and complex, and also turn on the technical and other capabilities of people and groups. I imagine an affordance approach, which I propose and briefly showcase here, would yield insights in these other areas as well.

A. Political Affordances

Democracy is set up, in theory, to make politicians affordances for their constituents. Perhaps the most obvious way citizens of a democracy could influence surveillance policy would be to elect reform minded leaders. You would think that a concerted enough effort here could substantially change the way we balance national security against civil liberties in the United States. And indeed, Congress recently took the occasion of the sunset (by statute) and invalidation (by the U.S. Court of Appeals for the Second Circuit) of the bulk collection of American phone data by the National Security Agency as occasion to require more process before the agency can access these records.[28] 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.[29] This story says that American preferences are diffuse across the population and weakly held. Whereas the interests of the intelligence community, public and private, are very intense; that community is highly motivated and close to the levers of power. 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 they are relational by organism, we might say that the political process is a perceived but false affordance for citizens but a very true affordance for special interest.

Public choice has some explanatory power in privacy law. Among the most careful and extensive examinations of attempts to achieve privacy through the political process comes from Priscilla Regan.[30] She looks at several case studies—including wiretaps and computer databases—in an

---

http://cvdazzle.com/.

[28] The case invalidating Section 215 of the Patriot Act under which authority the NSA was engaging in bulk collection is *ACLU v. Clapper*, Docket No. 14-42-cv (2nd Cir. 2014).

[29] For an early and influential discussion, see James M. Buchanan and Gordon Tullock, The Calculus of Consent: Logical Foundations of Constitutional Democracy (1962).

[30] Priscilla Regan, Legislative Privacy: Technology, Social Values, and Public Policy (1995).

effort to unpack the various policy dynamics behind federal lawmaking. Regan observes that, in each instance she examines, vested interests win out over privacy advocacy. She concludes that for meaningful change to occur we will need to elevate privacy as a substantive societal value as well as wait patiently for a "policy window" in which to act.[31]

But the issue is still more complex. Politicians are true affordances for citizens to the extent they have affordances themselves, i.e., 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 they are not so positioned. With respect to national intelligence, specifically, political scientist Amy Zegart discusses why Congressional oversight of the executive branch remains elusive even in the face of statutory schemes that provide for it.[32] She points in particular to politicians' lack information about surveillance programs and, more importantly, the expertise to assess the information they have. As Zegart puts it, "expertise is critical and always in short supply."[33]

As discussed above, design theorist William Gaver introduces the concept of a *nested* affordance, by which he means affordances that lead to others.[34] Sociologists Jennifer Earl and Katrina Kimport offer the concept of *leveraged* affordances to describe digitally enabled social change.[35] Their context is technology but the insight is just as 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 themselves in a particular domain, then no degree of responsiveness creates an affordance in the citizen.

B. Legal Affordances

Elected officials are not the 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

---

[31] *Id.* at 199.

[32] Amy B. Zegart, *The Domestic Politics of Irrational Intelligence Oversight*, Poli. Sci. Q. 126:1 (2011).

[33] *Id.* at 9. This claim in line with what other scholars have observed, including within this volume. Additional issues include the lack of visibility (and hence, credit) of good stewardship and extreme risk aversion, should terrorist activity actually occur.

[34] *See supra* note 11.

[35] Jennifer Earl and Katrina Kimport, Digitally Enabled Social Change (2011).

the Constitution, including those provisions, such as the First Amendment's dictates around speech and assembly or the Fourth Amendment warrant requirement, that implicate surveillance. The states also have constitutions, some of which mention privacy directly.[36]

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

This is true for a few reasons. One has to do with 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, i.e., where the monitoring of a person or group by the government was extensive enough to implicate free speech, the citizen must show that he is being watched in fact, and that this monitoring is chilling his ability to assemble or to express himself.

This turns out to be difficult, in part because much surveillance occurs in secret, so that litigants cannot show they are being watched in fact, and in part because of the implication that the very act of suing can be evidence that a litigant has not been cowed. Thus in *Laird v. Tatum*, 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."[37] But the Court ultimately held that the petitioner before it was not chilled. Indeed, the petitioners "cast considerable doubt on whether they themselves are 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…[38]

In the Fourth Amendment context, the citizen must show that her own, reasonable privacy interest has been unreasonably invaded in the exact right way. Until very recently, the citizen could not challenge a statue facially under the Amendment, unless it was to cure a defect in a warrant clause.[39]

---

[36] *E.g.*, C.A. Const. art. 1 § 1 (listing the pursuit of privacy as among citizens' "inalienable rights").

[37] Laird v. Tatum, 408 U.S. 1, 11 (1972).

[38] *Id.* at 13 n.7 (discussing how the aggressive litigants at bar are clearly "uncowed").

[39] *See* Sibron v. New York, 392 U.S. 40 (1968), abrogated by City of Los Angeles v.

He still cannot sue over the invasion of another's interest, even where the evidence obtained unlawfully is introduced against him in court.[40] The recourse of a mother of a defendant who was jailed because the police broke into her apartment and found evidence against him would be limited to tort, which the Court "has failed to nurture and at times affirmatively undermined."[41] 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 life. It is often easier for law enforcement to ask Google or AT&T for your web history instead of you. And, generally speaking, the law has treated 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. This tendency in the law is known, and sometimes lamented, as the "third party doctrine."[42]

Another, simpler reason courts afford less recourse is that unsympathetic and under-resourced defendants make unfortunate champions for the rest of society. The point is controverted, but it seems clear at one level that many of 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 wind up with the affordances of the accused criminal, in certain respects our lowest common denominator.[43]

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 criminal defendants are particularly well suited to push back against surveillance. Not according to Akhil Amar, who offers 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."[44] The criminal is not

---

Patel, 576 U.S. ____ (2015).

[40] *E.g*., United States v. Salvucci, 448 U.S. 83 (1980) (defendants lack standing to challenge unlawful search of their mother's house).

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

[42] For a discussion, see Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 528-29 (2006).

[43] Amar, *supra* note 41, at 796 (The criminal defendant is a kind of private attorney general. But the worst kind."). Of course, as Fyodor Dostoevsky said, "You can judge a society by how well it treats is prisoners."

[44] *See* Amar, supra note 40 at 796.

sympathetic, for instance, and often litigates bad facts, heedless of what this will do to Fourth Amendment precedent in general. The accused criminal rarely has access to a good lawyer. And so on.

Also skeptical is Shima Baradaran, who points out that courts side with the state over defendants in the overwhelming (4/5) majority of Fourth Amendment cases.[45] 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. Thus, courts engage in "blind balancing" that almost invariably inures against the criminal defendant and, by extension, to innocent citizens whom the Fourth Amendment also avowedly protects.[46]

There are many more ways in which citizens hoping to achieve reform through the courts are stymied. And there are 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 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. Technical Affordances

The last two sections focus, respectively, on the capacity of individuals to restrain government through legislatures and courts. As Lessig's interlocutors remind us, individuals and firms have technical means for resistance as well.[47] For 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 technical affordance in that it affords hiding. Very good hiding: over-the-counter encryption, so to speak, apparently can thwart very sophisticated attempts to access protected content.[48] Encryption is very promising. It is a technical

---

[45] Shima Baradaran, *Rebalancing the Fourth Amendment*, 102 Geo. L. Rev. 1 (2013).

[46] *Id.* at 3.

[47] *See, e.g.*, Tim Wu, *When Code Isn't Law*, 89 Virginia L. Rev. 679 (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).

[48] *See* Adrian Covert, *iOS Encryption is So Good, Not Even the NSA Can Hack It*,

affordance that is available to most and does not necessarily rely upon the good will of third parties. Encryption is no panacea, however, and 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 isn't. A few years ago computer scientist Alma Whitten and electrical engineer J.D. 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."[49] They found, famously in computer security circles, that what makes for usable software in general does not suffice when it comes to security. Their test subjects made errors and, as a consequence, did not actually hide what they were saying.

A much more recent paper looks at the technical affordances of a particular population for whom secrecy and discretion is 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.[50] Like Whitten and Tygar, this team found that existing technology was still not usable. Further, available technology tended to "actively interfere with other aspects of the journalist process" such as the verifiability of sources and source information.[51] This despite the fact that journalists are commonly identified as the very people who need heightened computer security to accomplish their important work.

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 still must 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 all the government can see is the direction and frequency of traffic, so-called "metadata," the computer science is

---

Gizmodo (Sept. 13, 2012) (noting that the newest version of the popular iPhone has very good encryption), online at http://gizmodo.com/5934234/ios-encryption-is-so-good-not-even-the-nsa-can-hack-it.

[49] Alma Whitten and J.D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*, Proc. of the 8th Ann. USENIX Security Symposium (1999).

[50] Susan E. McGregor et al., *Investigating the Computer Security Practices and Needs of Journalists*, Proc. of the 24th Ann. USENIX Security Symposium (2015). USENIX is the premiere academic symposium on computer security.

[51] *Id.*

increasingly clear that it may still make guesses as to the content.[52]

Among the most promising developments for privacy enthusiasts following the revelations of CIA contractor Edward Snowden has been the decision of Apple, Google, and other companies to encrypt communications by default. Defaulting to encryption obviates the above problems—something that is already on need not be usable and most people stick with defaults, making encryption widespread.[53] 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 law enforcement is usually after, and firms have the resources to fight government surveillance of their customers. Indeed, the Snowden revelations and subsequent global reaction to the NSA spying capabilities have invigorated privacy as a competitive differentiator. Firms are making technical changes, discussed above, and pushing back against subpoenas with greater force.

Just as governments can leverage the market as a modality of regulation, e.g., by increasing taxes on undesirable behavior, so can the citizen pool his affordances through the market to pressure larger, organized firms to press her interests. This could be thought of as an instance of nested or sequential affordances, group affordance, or something else. By whatever label, we cannot answer the question of 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 Jack Balkin, Jon Michaels, and others argue, the best way to characterize the past relationship between governments and corporations around surveillance is *synergistic*.[54] Firms use government-mandated data and governments leverage private databases and tools. Both government and firm activities erode societal expectations of privacy.

---

[52] *E.g.*, Shahram Mohrehkesh et al., *Demographic Prediction of Mobile Use from Phone Usage*, Mobile Data Challenge 2012 (by Nokia) Workshop (June 18-19, 2012).

[53] Of course, the price of liberty is eternal vigilance. Today, law enforcement is actively reigniting the battle over backdoors by arguing that the FBI and others should have access to keys that unlock all encryption when necessary.

[54] Jon D. Michaels, *All The President's Spies: Private-Public Partnerships in the War on Terror*, 96 Cal. L. Rev. 901 (2008); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1 (2008).

Very recent work by Avidan Cover examines whether, as some argue, companies can nevertheless stand in the shoes of individuals and assert privacy claims on their behalf.[55] Cover concludes that corporations seldom push back against the government in practice, and when they do, they are hamstrung by a variety of forces. 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.[56] Cover also takes issue, normatively, with the idea that citizens should have to rely upon companies to press their freedoms—especially in light of the role British companies played in the perceived abuses of colonial America.

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 the preference will be respected. It might not be, because, if you think about it, it would be the same government asking for the data to enforce the failure to resist.

Take the respective privacy policies of two companies that store and analyze consumers' genetic information. The company 23andMe says in its policy that if it gets a lawful request for genetic information it will turn that information over to the government: "Under certain circumstances your information may be subject to disclosure pursuant to judicial or other government subpoenas, warrants, or orders, or in coordination with regulatory authorities."[57] 23andMe's competitor, Navigenics, also acknowledges the prospect that the government may seek to compel disclosure but, unlike 23andMe, commits to "use reasonable and lawful efforts to limit the scope of any such legally required disclosure."[58]

For the many civilian-consumers who worry about privacy, this would seem to suggest Navigenics is the better choice for personalized genetics. But what happens if Navigenics decides not to push back as advertised?

---

[55] 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 (2009).

[56] This occurred when Congress conferred retroactive immunity on Internet service providers that cooperated with the NSA through passage of the FISA Amendments Act of 2008.

[57] 23andMe Privacy Policy, online at https://www.23andme.com/about/privacy/?version=3.4.

[58] Navigenics Privacy Policy, online at https://www.navigenics.com/visitor/policies/our_policies/privacy/.

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 or state equivalents. The FTC can bring an enforcement proceeding under its authority to police against deceptive statements.[59] 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 tends to hollow out this particularly 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 properly motivated. That motivation appears to be mounting in the form of domestic and, to a large degree, international pressure on American firms to put citizen-consumer privacy first.

III. AFFORDANCES AS 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, technical, and other avenues to resist or effectuate change. But many of these affordances turn out to be false or compromised upon inspection. Citizens can vote officials into office who care about privacy but those officials lack the capacity for real oversight. Citizens have technical means by which to resist surveillance but the technologies lack usability and can turn the citizen into a target. Citizens can extract promises from firms to push back against surveillance on their behalf but 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 this year and companies have shown an interest in pushing back against demands for consumer data.[60] Recent case law is particularly promising. In a series of Fourth Amendment decisions, the Supreme Court has shown a willingness to interpret the Constitution if not more broadly, then more favorably.[61] This very term the

[59] Federal Trade Commission Act, 15 U.S.C. §§ 41-58.

[60] Among other things, the USA Freedom Act requires ISPs to store telephone records instead of the NSA and makes the Foreign Intelligence Surveillance Courts from which the NSA seeks approval for its activities more adversarial. USA Freedom Act of 2015.

[61] Various majority opinions have in a sense narrowed the case law in places by tying it so closely to the common law tort of trespass. E.g., United States v. Jones, 565 U.S. ___ (2012) (affixing a GPS to a car requires probably cause); Florida v. Jardines, 569 U.S. ___

Court repudiated its prior holding that Fourth Amendment cases were too fact bound to accommodate a facial challenge, allowing a hotel owner to challenge a statute that gave police access to visitor logs.[62] Another recent decision recognized the intimacy and extent of data we keep on our personal devices and clarified that officers could not search a smart phone merely incident to arrest and without a warrant,[63] which some commentators believe paves the way toward a reexamination of the third party doctrine.[64]

What do these and similar developments mean for our title concern? Will we now reach a state of equilibrium between privacy and competing values? Because presumably the tolerable—let alone optimal—degree of government surveillance of citizens is not zero, or any specific number. We cannot refer to dollars spent or point to a particular year that was just fine for privacy. Ask citizens and you get different answers. Some other benchmark must obtain.

In answering these difficult and complex questions, 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 effect on the affordances of everyday citizens. If we are ever able to document that people have real means to resist and reform government surveillance, but still chose not to do so, then the 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 posed the important but under-examined question of whether Americans have the means by which to resist and reform surveillance. It then introduced the concept of affordances to help structure an answer that question. The essay made three contributions in so doing. First, it suggested 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 is itself a kind of affordance. Second, the essay examined surveillance affordances of various kinds—political, legal, technical, and

(2013) (bringing a drug-sniffing dog onto private property requires probable cause).

[62] City of Los Angeles v. Patel, 576 U.S. ____ (2015).

[63] Riley v. California, 573 U.S. ___ (2014).

[64] *E.g.*, Ryan Watzel, *Riley's Implications for Fourth Amendment Protection in the Cloud*, 124 Yale L.J. F. 73 (2014) ("[W]hile failing to explicitly afford 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…").

market—and in each instance found limits to otherwise viable avenues of resistance and reform. Finally, the essay proposed 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.