On the incommensurability of laws and technical mechanisms: Or, what cryptography can't do

Joan Feigenbaum[1] and Daniel J. Weitzner[2]

[1] Computer Science Department, Yale University, New Haven CT, 06520 USA, joan.feigenbaum@yale.edu
[2] Internet Policy Research Initiative, Massachusetts Institute of Technology, Cambridge MA, 02139 USA, weitzner@mit.edu

Abstract. We examine several technology-policy debates in which technical and legal perspectives are so at odds that they approach incommensurability. Investigating the use of digital rights management systems in the online-copyright debate and the dispute over the impact of end-to-end encryption on lawful surveillance, we offer an analysis of the source of this incommensurability. In these two policy debates, both sides invoke the rule of law to support their position, but in each case they draw selectively from the constituent parts of the rule of law, resulting in seemingly irreconcilable differences. We show that the rule of law is actually composed of rules (susceptible to deterministic evaluation against a set of facts) and principles (expressing important values but not susceptible to purely formal evaluation). The clash between rules and principles exacerbates the difference in perspective between system designers, who favor formal rules, and policy makers, who are more comfortable with situational application of principles. Following our observation that the rules-principles gap makes for incommensurate debate between legal and technical actors, we identify steps that each discipline can take to move toward more coherent policy for the networked, digital environment.

1 Introduction

With the rise of the Internet and other globally deployed technical infrastructures, we have seen frequent clashes between claims of legal and policy experts about how technical systems ought to behave and claims of architects and engineers of technical systems about what type of system behavior is both possible and desirable. At the root of these disputes, one often finds incommensurate views about what it would mean for a system to "work," *i.e.*, to actually "solve" a real-world problem. Generally speaking, a technical system is judged to have succeeded if it provides a *fully specified, correct solution* to a *well defined and well understood problem* and is *implemented and maintained according to sound engineering practice*. By contrast, legal regimes are judged according to very different standards. A proposed law or regulatory framework is judged successful if its constituent rules are *proper expressions of the society's values* and have the necessary *indicia of legitimacy*.

In this paper, we examine this design incommensurability in the context of the socio-technical debate about encryption and surveillance. Our goal is to arrive at legal and technical design principles that lead to the development of technology that complements applicable laws and promotes society's values. Here, we begin by presenting the criteria by which legal regimes are judged. We then briefly revisit another socio-technical domain in which the incommensurability of law and technology led to stalemate, *i.e.*, digital rights-management (DRM) systems. Finally, we offer two technical and legal design patterns and discuss their potential for moving the debate forward and achieving our long-term goal.

2 Related work

Many cryptographers, computer-security researchers, law-enforcement officials, and others in both the legal world and the technical world have remarked upon the tension between law and technology in the area of surveillance. Much of the discussion focuses either on the technical aspects or on the legal and human-rights aspects of the issue. We take a cross-disciplinary approach by providing what is, to the best of our knowledge, the first *structural* jurisprudential explanation for this tension. We now briefly review the main positions that have been taken on the question of encryption and surveillance.

At one end of the spectrum is the view that the technical community is simply thwarting the lawful exercise of warrants and court orders authorized by statute and the relevant basic law: the Constitution in the case of the United States. Under this view, the tension is resolved by the fact that both individuals and organizations are obligated, under the All Writs Act [9] in the US and similar laws in other democratic countries, to provide necessary assistance to government agencies in the execution of warrants and, more generally, in "the proper administration of justice." Hennessey and Wittes [8] give good explanations of both the All Writs Act and this general view of the tension between law and technology. A related position is given in detail by Rozenshtein [15], who explicitly rejects "technological unilateralism" of the type endorsed by crypto maximalists. Rozenshtein draws our attention to the technical and political centrality of *surveillance intermediaries* such Google, Facebook, and other large-scale Internet platforms.

Certainly the All Writs Act obligates individuals and organizations to assist the government in the administration of justice; however, because the scope of assistance subject to mandate under the Act is far from settled, it does not fully resolve the tension between lawful surveillance and end-to-end encryption as a legal matter. In the FBI vs. Apple case [9], for example, Apple's claim that complying with the US government's order to develop the software needed to unlock a dead terrorist's iPhone represented an "undue burden," that it put the security of Apple's operating-system software at risk for all Apple users, and that it violated Apple's First Amendment rights against compelled speech inasmuch as the Government sought to require Apple to write new software was vigorously debated and never resolved in court. Beyond the specific requirement

proposed by the government in the case, Apple's concern that there may be unacceptable cybersecurity risks created by some proposed exceptional access requirements are well substantiated. Once a technical capability is built into a system, there is always a possibility that it will be misused. History demonstrates that this is not a hypothetical possibility; in the Vodaphone Greece scandal [14], for example, a wiretapping capability mandated by United States law was used against Greek government officials. In summary, a general legal obligation to assist the government does not answer the question of what specific assistance is required in a given case, nor does it provide definitive guidance on the broader policy question about what obligations, if any, ought to be imposed on service providers with respect to encryption.

At the other end of the spectrum, there is the view that governments, including democratic ones, routinely violate privacy rights. Because privacy is a fundamental human right, the tech community is therefore morally obligated to build user-friendly strong encryption into as much of the computing and communications infrastructure as possible and *not* to build anything that facilitates governments' decrypting any user's data against that user's will. In response to the Snowden revelations, a large group of distinguished cryptographers and computer-security researchers wrote [2]:

> Indiscriminate collection, storage, and processing of unprecedented amounts of personal information chill free speech and invite many types of abuse, ranging from mission creep to identity theft. These are not hypothetical problems; they have occurred many times in the past. Inserting backdoors, sabotaging standards, and tapping commercial data-center links provide bad actors, foreign and domestic, opportunities to exploit the resulting vulnerabilities.

Schneier [10] adheres to this view, emphasizing that, since the 9-11 attacks, there has simply been far too much mass surveillance and that the only logical response is mass encryption. A more general theory of the morality of encryption is given by Rogaway [16]. Once again, we believe that, while there is a great deal of truth in this view of the situation, it does not satisfactorily resolve the question of how to accomplish *lawful* surveillance in a mass-encryption world. In response to government agencies' fear that perfectly legal surveillance, authorized by judicial warrants and viewed by most of the public as a legitimate tool in the fights against crime and terrorism, could become ineffective if most of what it yields is ciphertext for which decryption keys are unavailable, the proponents of ubiquitous encryption simply say "find other ways to get the data." Some point out that the warrants in question grant only the authority to intercept a communication or to seize a device; they don't guarantee that the sought-after information will be found in the communication stream or on the device – or that it can be decrypted if it is found in encrypted form.

None of this is to say that these commentators are anarchists or that they reject the rule of law. To the contrary they often invoke the rule of law as motivation for their views. They just seem to have lost confidence in the effectiveness of the legal system's ability to provide an adequate level of privacy protection.

Orthogonal to these two legal and policy claims is a set of technical arguments about the risks that mandated exceptional access poses to the global information and communications infrastructure used by billions of people around the planet. A number of proposals for exceptional-access systems create serious security risk. Once those exceptional-access mechanisms are installed for law enforcement, the private communications of all other users also become more vulnerable to attack by malicious criminals and terrorists. Exceptional access for law enforcement means storing the secret keys to communications and data around somewhere, possibly for months or years, to enable police to gain access when they need it. Such a design forces security technologists to backtrack on lessons learned over the years about how to design systems [1].

> Exceptional access would force Internet system developers to reverse forward secrecy design practices that seek to minimize the impact on user privacy when systems are breached. The complexity of today's Internet environment, with millions of apps and globally connected services, means that new law enforcement requirements are likely to introduce unanticipated, hard to detect security flaws.

This is a general summary of a number of more specific critiques of exceptional-access systems provided over the years.

Recognizing that both sides in the polarized debate over this issue have made legitimate points, we seek to bring an alternative framing to the discussion and illuminate possible paths forward. Thus our contribution is orthogonal to the policy and technical positions that have been laid down. We recognize individuals' rights to privacy, companies' legitimate desires to serve their customers, and companies' obligations to assist governments in executing warrants, provided such assistance is legally justified and technically feasible. The extent to which all of these goals are compatible is an open question that is properly the subject of democratic debate, legal research, cryptography and security research, and tech-industry product design.

3 Rules vs. principles in legal regimes and the contrast with technical systems

The tension between technical and legal views of sensitive issues such as encryption and surveillance is illuminated by applying the jurisprudential lens. We are guided in our understanding of the incommensurability between technical systems and legal regimes by the work of Prof. Ronald Dworkin, the leading liberal scholar of western jurisprudence. Dworkin [5] shows that liberal legal systems, manifesting what is generally understood as "the rule of law," are actually composed of *both rules and principles*. Legal "rules" can be understood as logical propositions that are expected to yield answers about what is and is not permitted using formal reasoning capabilities. By contrast, legal "principles" articulate values and policies that must be reflected in a legal system but do not necessarily dictate an unambiguous outcome in any given case.

At first blush, one might think that laws should be commensurate in nature and structure with the logical rules expressed by computer code: formal statements that can be used to evaluate a given set of facts, yielding a determination about whether a given action is legal or not. However, in Dworkin's formulation, "rules" are only one component of "law." Rules are applied in a deductive fashion and yield a clear result. (That terms in a legal rule are sometimes vague and require further interpretation by legal authorities does not diminish their status as logical statements amenable to formal evaluation.) An example of a legal rule is:

> *If a person dies intestate, then her estate is passed down to her spouse and any surviving children.*

However, the rule of law also depends on a set of "principles." A principle is a "standard to be observed in the resolution of a legal dispute because justice demands it." It may also be a "policy that advances some social or economic goal." Dworkin offers two examples of principles:

> *(1) No one shall be permitted to profit from his or her own fraud.*
>
> *(2) In a society with such significant reliance on automobiles, the car manufacturer is under a "special obligation with respect to the construction, promotion and sale of his cars."*

Although both of these principles strike citizens of modern democracies as plausible and just, they are *not* ordinary legal rules. In particular, courts must apply these principles, but the result of doing so is not always clear. Courts generally do apply (1) in the disposition of a will. In a straightforward application, if an heir is found to have murdered the testator, he or she will not be allowed to inherit from the estate. However, Dworkin identifies many less straightforward applications in which the law *does* allow an individual to profit from fraud, *e.g.*, the law of "adverse position": If an individual occupies property illegally for some period of time without objection from the property owner, then the fraudster may successfully claim ownership of that occupied property.

Principle (2) regarding the obligations of automobile manufacturers is a *policy*, applied in certain cases to prevent a manufacturer from using a sales contract to limit its liability for harm from accidents. This principle was accepted by courts (in the days before more comprehensive automobile regulation) as superseding the ordinary law of contract. In applying this principle, courts showed themselves to be unwilling to apply legal rules in a mechanical fashion that would make them instruments of injustice or bad policy, as measured by principles such as those stated here.

Principles, in Dworkin's understanding, must be applied to certain legal disputes but do not necessarily yield a specific outcome. The scope of either (1) or (2) is neither clearly defined nor susceptible to mechanical application. In short, while principles are an essential part of the legal system, they do not function like rules. As principles are not subject to the same logically decidable evaluation as are rules, they cannot be applied in a manner that will necessarily yield a deterministic result.

Needless to say, the incorporation of principles that cannot be applied mechanically or counted upon to result in obviously "correct" outcomes is not what one expects as a component of technical-system design. Computer-system design certainly does have core principles (*e.g.*, "separation of policy and mechanism"), but the application of those principles in the context of a particular set of system requirements is supposed to result in a sound and complete system specification that can be translated into code. The difficulty of incorporating Dworkin's more complex and less deterministic notion of a "system" into the design and implementation of computer systems is in fact the crux of a number of currently unresolved disputes between computer scientists and lawyers.

3.1 Rules vs. principles in DRM

Digital rights-management systems were designed to enable digital distribution of copyrighted works while at the same time preventing unauthorized copying of those works. The designs were proposed to address the interests of copyright owners, who believed that the ease of making perfect digital copies of copyrighted works combined with the extremely low cost of (globally) sharing digital copies online would fatally erode the market for legitimate copies of digital works. Hence, rights holders sought to deploy DRM systems that prevented *any* unauthorized copying or distribution. In response, fair-use advocates rejected these systems, because they unduly restricted public access to copyrighted works.

Recall that US copyright law states that copyright owners have certain "exclusive rights," including the rights to reproduce the copyrighted work; to prepare derivative works; to distribute copies through sales, rental, lease, or lending; to perform the copyrighted work publicly; and to display the copyrighted work publicly. On the other hand, the law also stipulates that there are some exceptions to these exclusive rights: circumstances in which members of the public may make "fair use" of a copyrighted work, *i.e.*, reproduce, distribute, display, *etc.*, it without the permission of the copyright owner. Fair use, also known as fair dealing in some copyright laws, protects the public's ability to make limited use of copyrighted material for critical reviews, satire, and educational purposes, among other things. The copyright status of a piece of work is generally clear enough that it can be the subject of a rule, such as "this work may not be copied without permission." By contrast, the operations of fair use are not so easily defined. Copyright owners' rights form the basis of traditional "creative industries," and the "fair-use doctrine" is essential to the flourishing of scholarship, criticism, satire, and many other treasured forms of expression. In Dworkin's formulation, owners' exclusive rights are legal rules, and the fair-use doctrine is a principle.

The controversial nature of DRM technology is directly traceable to the inability of these systems to implement both the *rules* of copyright law together with the *principles* guiding the application of those rules. The primary design goal of DRM technology is to provide consumers easy access to copyrighted content while preventing *any* unauthorized copying. However, the goals of copyright law are broader than this goal inasmuch as the law also includes fair use and fair dealing. DRM systems should both protect owners' exclusive rights

(enforce the rules) and permit end users to make fair use (embody the principle). Unfortunately, current DRM technology is not able simultaneously to enforce copy-restriction rules and embody the fair-use principle. In mass-market content-distribution systems targeted at consumer-electronics devices, it is infeasible to give end users the technical ability to make fair use of copyrighted works without also giving them the technical ability to make arbitrary unauthorized use of the same works. Each DRM technology applies its own set of permissions and restrictions that do not, in fact, implement the rules of US or other national copyright law. So none of the technologies satisfies either copyright owners or fair-use advocates. We believe that this impasse perfectly captures the incommensurability of law and technology and that it is analogous to the impasse in encryption and surveillance.

3.2 Rules vs. principles in end-to-end encryption and surveillance

Since the Snowden revelations, the technology and law-enforcement communities have been in a pitched battle. Computer-security architects are pushing end-to-end encryption protocols further and further into the Internet, Web, and mobile communications infrastructure. In response, law-enforcement agencies from all over the world (US, UK, India, and Australia to name a few) have demanded that encrypted-communication systems be built to accommodate their ability to execute legally authorized surveillance. Why do so many people in the technical community feel the need to resist lawful government surveillance by technical means? As this is a socio-technical question, the current answer has both social and technical components. Alongside the question of how legal principles ought to apply to surveillance is the very real systems-security question of whether it is technically possible to build in "exceptional-access" capabilities without incurring unacceptable high security risks for other users [1]. While we are well aware of the importance of these systems-security questions, they are not the main focus of this paper.

From the technical community's perspective, the US government suffered a major loss of credibility as a result of the legally and morally excessive mass surveillance exposed by Snowden. In the words of Bruce Schneier [10], "the NSA has turned the Internet into a giant surveillance platform." More notably, wholly establishment figure Brad Smith (then General Counsel, now President of Microsoft) has defined the government as an Advanced Persistent Threat: Smith [12] wrote that the government-surveillance practices revealed by Snowden "threaten to seriously undermine confidence in the security and privacy of online communications. Indeed, government snooping potentially now constitutes an 'advanced persistent threat,' alongside sophisticated malware and cyber attacks." The solution, according to the conventional wisdom in the computer-security community as articulated by Schneier, is to recognize that "we have made surveillance too cheap. We have to make surveillance expensive again." Smith elaborates: "Many of our customers have serious concerns about government surveillance of the Internet. We share their concerns. That's why we are

taking steps to ensure governments use legal process rather than technological brute force to access customer data."

Smith's belief that governments should "use legal process ... to access customer data" provides a segue from the social and political aspects of the problem to the technical aspects. The Fourth Amendment of the US Constitution states that citizens have a right to be free from "unreasonable searches and seizures," a key source of the right to privacy. An extensive body of laws and court decisions provides guidance about what constitutes a "reasonable" search or seizure, *i.e.*, about when a government agent can get a warrant to violate a citizen's privacy.

Over time, the general privacy *principle* in the Fourth Amendment has been expressed as a set of more concrete *rules* in the form of electronic-surveillance statutes such as the Electronic Communications Privacy Act (18 USC 2701 et seq). Most other democracies have similar statutes. In Dworkin's terms, the "rule" is expressed in these statutes, establishing what procedures law enforcement has to follow to conduct electronic surveillance, how courts should consider those requests, and how citizens' rights will be protected in the operation of those rules. Today, with the combination of new technologies that enable a substantial expansion of surveillance power and the loss of trust from the Snowden disclosures, the technical community is standing up for privacy principles (as opposed to rules) by aggressively propagating end-to-end encryption. This proliferation of encryption technology is also, of course, just good security practice, but there has been an unmistakable and otherwise unexplainable growth in the use of end-to-end encryption throughout the public communications and information infrastructure since the Snowden revelations.

Just as there are privacy and civil-liberties protection principles at stake in the encryption debate, so too can law enforcement invoke principles beyond just the rules in surveillance statutes. Law-enforcement officials from the US, the UK, Australia, and elsewhere have all challenged the tech industry's decision to implement end-to-end, surveillance-resistant encryption on the grounds that such designs thwart the principle that companies have the obligation to assist in the execution of lawful court orders such as wiretap warrants. This principle does not have the weight of the Fourth Amendment or other fundamental rights, but it *is* established in law. As explained in Section 2, the leading example of this challenge from the law-enforcement community is the FBI's claim under the US All Writs Act that Apple should create a modified version of the security features in its iOS operating system to enable the FBI to unlock a phone used in the San Bernardino terrorist attack [8]. While there is a *general* obligation in US law to assist the government in fulfilling lawful court orders (such as search warrants), in this and other cases, US courts have declined to find that technology companies have an arbitrarily broad obligation.

As the debate over encryption and surveillance has played out. both technical and law-enforcement communities have made earnest but incomplete arguments. Law enforcement invokes the "rule of law" but comes closer to advocating for the "rule of rules." In its appeal to the obligation to assist the government in executing court orders, the government side seems to ignore both the historical

limits on that *rule* and to give short shrift to the importance of the *principles* associated with limiting the scope of government surveillance. By the same token, frequently heard arguments from the technical community cite the *principle* of privacy protection as a reason to refuse to design systems that might address law-enforcement needs, and thus place the principle of privacy protection above all other rules principles that are properly part of our rule of law framework. In neither case do we attribute bad faith to these two opposing communities. Still we can see that failure to account for the complete the role of both rule and principle in the rule-of-law system leads to incommensurate policy positions.

4 Design patterns that address the tension among rules and principles

We have shown that the incommensurability of the technical-design and legal-system perspectives arises from a failure to distinguish between rules and principles. Conflict and confusion between the technical and legal contours of rules and principles have repeatedly muddled both design decisions about technical systems and the effective operation of law in the digital realm. What's more, this confusion has created a nearly existential strain between the technical community and governments around the world. To help disentangle this confusion, we offer two design patterns that will bring greater clarity and engender progress in difficult digital-policy debates. The first is a challenge to the legal community to make rules clearer and to reduce the gray area between principles and rules. The second is a design goal for the technical community, *i.e.*, to design systems with increased transparency and accountability, thus enabling an open dialogue about how legal principles should operate in new contexts.

4.1 Socio-Technical Design Pattern #1: Reduce the gray area between rules and principles

When the resolution of a legal question depends on both the evaluation of a rule (something computer systems can do well) and application of a principle (something that is generally undecidable for any logical system), confusion follows. DRM systems are controversial because they are designed to give effect to a set of rules that reflects neither the full range of the law nor the full operation of fair-use principles, producing a result that appears unjust. When surveillance rules appear to accord governments intrusive power beyond what principle says they should have, then some system designers take matters into their own hands.

Clarifying rules and narrowing the cases in which principles have to enter into the evaluation of surveillance authority would bring stability and increased trust to surveillance law. In most countries, electronic-surveillance rules are decades old (with the notable exception of the UK) and fail to account for the substantial intrusive power associated with many new technologies that extend the reach of both government and commercial surveillance. As an example of how the gray area between rules and principles might be reduced, consider the question of how

law enforcement is able to gain access to location information in the course of a criminal investigation.

Location privacy is one of the more contentious privacy and civil-liberties issues in the United States. The underlying technology has changed dramatically, and there is significant contention about how rules and principles ought to be understood in determining how law enforcement can access this very sensitive data. To begin with, in the years since cell phones first became popular, mobile communications devices have incorporated hardware and software that reveal the real-time location of most individual users. Courts trying to decide what rules should govern law-enforcement access to location data have generally settled on a 1994 law that was written not to cover location data but rather to protect the privacy of email and web-browsing logs (18 US Code 2703(d)). This rule conditions police access to data on the ability to present a court with "specific, articulable facts" showing that the information sought is relevant to an ongoing criminal investigation. This particular standard is a much higher burden for the police to meet as compared to what they have to demonstrate to get access, for example, to a target's bank-account information. Yet it is lower than the full "probable-cause" standard required by the Fourth Amendment of the US Constitution for wiretaps and other access to "content" such as email.

Conflicting views of how privacy principles ought to shape rules for location access has left the current rule under attack by both law enforcement and civil-liberties advocates for alleged violation of Fourth-Amendment principles. Civil libertarians claim that it under-protects privacy for failing to extend full Fourth-Amendment probable-cause protection to citizens' location information. On the other hand, law enforcement invokes yet another constitutional principle known as the "third-party doctrine." This principle [17] provides that, when an individual voluntarily surrenders personal information to a third party, he or she has waived privacy interest in the information, and therefore no warrant is required. Law-enforcement officials argue that this principle applies, because mobile-phone users have voluntarily transmitted their location information to mobile-network operators and thus waived any privacy interest in it. Civil libertarians argue that location data is highly sensitive and deserves protection from government intrusion notwithstanding the fact that third parties such as mobile network operators or Internet platforms handle that data.

This tangle of rules and conflicting principles has brought the dispute to the United States Supreme Court twice. The first case, United States v. Jones [19], failed to resolve the underlying dispute with certainty, but it indicated that access to historical location data (records of past locations) over a long period of time (28 days) was a privacy intrusion. The Supreme Court is expected to issue another decision in this area shortly.[3] While this debate continues in the

[3] Note added in July 2018: On June 22, 2018, the Supreme Court ruled [4] that historical location data is subject to full Fourth-Amendment privacy protection, rejecting a lower-court decision [18], which had found that, in some circumstances, the police could access location data even without the traditional Fourth-Amendment proof of probable cause. Although it is an important step forward for privacy protection,

legal system, computer-system designers face legitimate questions about whether they should be building tools that help users obscure their location data from law enforcement or rather defer to the legal system to protect privacy. The gray area created by an inconsistent combination of rules and principles could stand to be clarified and simplified with a straightforward set of legal rules that address *all* aspects of location privacy, as opposed to just those aspects addressed in the Carpenter case that the Supreme Court is now considering [4].[3] This would increase confidence in the legal system and reduce the perception that the only way to protect privacy is through unilateral action by technologists. Of course, computer security is an important component of privacy and thus a responsibility for all system designers, but we should not have to rely on technical means alone. Privacy protection is a fundamental responsibility of the legal system in democracies.

In addition to location information, there are numerous security and privacy rights at risk that remain unprotected under law. Just to name a few, we need more clear rules governing the privacy and law-enforcement access conditions of personal data collected by new "smart-city" technology, travel patterns revealed by automatic license-plate readers, and data collected an analyzed by in-home listening devices such as the Amazon Echo and Google Home. All of these technologies raise pressing privacy questions. The legality of many such privacy issues is decided in a tangle of principle and rule. To the extent possible, we should narrow these gray areas and work toward explicit privacy rules. This will increase user trust and reduce the burden on technical designers to solve problems that more properly belong in the legal sphere.

4.2 Socio-Technical Design Pattern #2: Bring transparency and accountability to the operation of principles

The legitimacy of the legal system depends on the ongoing and transparent application of principles alongside the adjudication of specific rules. Technical mechanisms that bring more comprehensive transparency and accountability serve two important functions. First, systems that function with more complete transparency enable fact-based consideration of whether laws are working properly, addressing the democratically desired balance of interests. Second, accountable mechanisms [6] increase public confidence that laws are actually being followed by enabling citizens and their representatives both in government and civil society to monitor the application of law to the operation of systems, pointing out and seeking remedies when violations of rules occur.

Transparency is vital to sound technology development, because so little is known about how new systems work and how they affect society's values. Systems with better transparency properties could help provide policymakers and the public with a sound basis on which to make surveillance policy and with adjustments to privacy, security, and law-enforcement needs based on actual facts

[3] the Carpenter decision still leaves open numerous digital-privacy questions, including what standard of privacy protection the United States Constitution provides for real-time location data.

about how systems behave in public. A variety of cryptographers including [7] have shown designs of cryptographically sound systems that provide comprehensive statistics on surveillance operations without disclosing details of specific law enforcement investigations. The debate over encryption and surveillance is a classic example of one in which more transparency about actual system operation is needed. Since 2014, when then-FBI Director James Comey called for Internet companies to redesign their systems to assure law-enforcement access to encrypted content, facts about the surveillance environment have been in short supply. As law enforcement claims substantial harms to investigations due the end-to-end encryption on mobile devices, there have been questions about the actual magnitude of this harm. For some time, the FBI claimed it was having trouble quantifying the impact of encryption, then claimed that encryption hampered investigations in more than 7000 mobile devices. But in the end, the actual number appears to have been closer to 1000 [3]. This is just one area in which more technical contribution is necessary to bring increased trust to the online environment. Lack of transparency leads to distrust and efforts to achieve protection through purely technical, rather than legal, means.

Accountability in the operation of surveillance systems is also vital to public trust and good governance. When surveillance systems seem to operate in an opaque fashion, the public in general and the technical community in particular feel that the broader principles of privacy protection and limited government power over citizens' liberty are left legally unprotected. Building accountable surveillance systems requires formal statements of what surveillance has been authorized, reliable logging mechanisms, and appropriate deployment of secure computation techniques and zero-knowledge proofs that provide guarantees of lawful behavior without disclosing sensitive information about ongoing law-enforcement investigations. Several such designs [7] [11] have now been proposed, but much more work is required to bring full accountability to information usage and surveillance.

While we exhort the policymakers to disambiguate principles and carve out the elements that can be turned into rules whenever possible, there will always be circumstances in which the application of rules to a set of facts is incomplete or undecidable without the broader contribution of legal principles. That is certainly the case in the intersection of powerful new information technologies with fundamental rights such as privacy or free expression. Hence, system designers ought to consider how to bring greater transparency and accountability [20] to the design and operation of their systems, and policymakers ought to put requirements for greater transparency into the law.

5 Conclusion

We have observed that some in the cryptology research community believe that the only effective way to support privacy principles is to deploy end-to-end encryption capabilities as widely as possible. As we have shown, we understand this stance to reflect the belief that the legal system has failed to respond ap-

propriately to the spread of new surveillance technologies and otherwise abused its authority. Legal rules in place are inadequate to protect privacy in the face of powerful new surveillance techniques. Building technical work-arounds to protect users from inadequate legal privacy protection is an understandable stance and may be justifiable in the near term. But surveillance-avoidance technology alone will not create the kind of privacy-respectful society called for by our democratic values. On the technical side, we should broaden efforts to build more transparent, accountable systems. These systems will help provide the public with information necessary to assure that the legal system strikes the right balance between legal rules and applicable principles. The obligation on the law and policy community is to shrink the gray areas where unclear or outmoded rules leave privacy principles unprotected. With the increased sense of trust that a more transparent, accountable environment brings, it should also be possible to re-create a more cooperative relationship between the technical and law-enforcement communities, so that the police have the tools and expertise necessary to protect society, and citizens are confident that the law ensures that privacy will be protected, both as a matter or rule and principle.

Acknowledgements

Feigenbaum was supported in part by US National Science Foundation grants CNS-1407454 and CNS-1409599 and by the William and Flora Hewlett Foundation grant 2016-3834. Weitzner was supported in part by the William and Flora Hewlett Foundation grant 2014-1601.

References

1. Abelson, H., Anderson, R., Bellovin, S., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P., Rivest, R., Schiller, J., Schneier, B., Specter, M., Weitzner, D.J.: Keys under doormats: mandating insecurity by requiring government access to all data and communications. J. Cybersecurity. **1**, 69–79 (2015). `https://doi.org/10.1093/cybsec/tyv009`
2. An Open Letter from US Researchers in Cryptography and Information Security, January 24, 2014. `masssurveillance.info`
3. Barrett, D.: FBI repeatedly overstated encryption threat figures to Congress, public. Washington Post (May 22, 2018).
4. Carpenter v. United States, No. 16-402, 585 U.S. — (2018).
5. Dworkin, R.: Taking Rights Seriously. Harvard University Press, Cambridge (1978)
6. Feigenbaum, J., Hendler, J., Jaggard, A., Weitzner, D.J., Wright, R.: Accountability and deterrence in online life. In Proceedings of the 3rd International Web Science Conference. Article no. 7. ACM, New York NY, USA (June 2011). doi: 10.1145/2527031.2527036
7. Frankle, J., Park, S., Shaar, D., Goldwasser, S., Weitzner, D.J.: Practical Accountability of Secret Processes. In: Proceedings of the 27th Security Symposium. USENIX, Berkeley CA, USA (August 2018)

8. Hennessey, S., Wittes, B.: Apple is selling you a phone, not civil liberties. Lawfare. (February 18, 2016). https://lawfareblog.com/apple-selling-you-phone-not-civil-liberties
9. In re Search of an Apple iPhone, 2016 WL 618401.
10. Jackson, J.: Security expert seeks to make surveillance costly again. Computerworld. (November 7, 2013). https://www.computerworld.com/article/2485721/data-security/security-expert-seeks-to-make-surveillance-costly-again.html
11. Kroll, J., Felten, E., Boneh, D.: Secure protocols for accountable warrant execution. Working paper. https://www.jkroll.com/papers/warrant_paper.pdf
12. Meisner, J.: Protecting customer data from government snooping. Microsoft Technet: The Official Microsoft Blog. (December 4, 2013). https://blogs.technet.microsoft.com/microsoft_blog/2013/12/04/protecting-customer-data-from-government-snooping/
13. Pato, J., Paradesi, S., Jacobi, I., Shih, F., Wang, S.: Aintno: Demonstration of information accountability on the web. In: Proceedings of the 3rd International Conference on Privacy, Security, Risk, and Trust and 3rd International Conference on Social Computing. pp. 1072-1080. IEEE Computer Society, Los Alamitos CA, USA (October 2011)
14. Prevelakis, V., Spinellis, D.: The Athens Affair. IEEE Spectrum. **44:7**, 26–33 (2007). doi: 10.1109/MSPEC.2007.376605
15. Rozenshtein, A.J.: Surveillance Intermediaries. Stan. Law Rev. **70**, 99–189 (2018).
16. Rogaway, P.: The Moral Character of Cryptographic Work. Cryptology ePrint Archive, Report 2015/1162 (2015). https://eprint.iacr.org/2015/1162.
17. Smith v. Maryland, 442 U.S. 735 (1979).
18. United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016).
19. United States v. Jones, 565 U.S. 400 (2012).
20. Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., Sussman, G.: Information Accountability. Comm. ACM. **51:6**, 82–89 (June 2008). doi: 10.1145/1349026.1349043