A HOOVER INSTITUTION ESSAY

International Spillover Effects

THE US ENCRYPTION DEBATE

JENNIFER DASKAL

Aegis Paper Series No. 1611

With companies like Apple, Facebook, Google, Microsoft, and other major communications providers increasingly offering default and end-to-end encryption of mobile devices, smartphone operating systems, and a range of communications products, the domestic encryption debate is heating up. On the one hand, civil libertarians, human rights defenders, and a range of intelligence officials praise these developments as a way to keep private communications private, protect against cyberespionage and cyberterrorism, and enable dissidents and human rights activists to build social networks and operate more safely under repressive regimes.[1] On the other hand, FBI director James Comey and other state and federal law enforcement officials increasingly warn that law enforcement is "going dark"—referring to the inability to access communications or other data in a readable form.[2]

At the same time that default and end-to-end encryption enables dissidents to communicate, it also enables terrorists and other criminals to plot and plan without fear of detection. It means that even when a judge signs off on a warrant based on probable cause to believe that a particular device or account contains evidence of a crime that has been or is about to be committed, law enforcement cannot unlock the smartphone or obtain the relevant data in readable form. The concern is that criminals may go free, and dangerous plots may be left undetected. Comey and other law enforcement officials want US-based companies to provide sought-after data in readable form—and to maintain the technological capacity to do so.[3] But the approach is controversial; a powerful coalition of companies, civil liberties groups, and many others decries such efforts at mandated access as undercutting security for us all.

This is a domestic debate with global reach. (It is also a debate that is playing out simultaneously in other nations as well.) The Internet, after all, is a global system; US-based companies operate multinationally and sell their products around the world.

Jennifer Daskal is an associate professor of law at American University's Washington College of Law, currently on leave at as an Open Society Institute Fellow. Special thanks to Ben Wittes, Jack Goldsmith, Jane Chong, and the Hoover Working Group on National Security, Law, and Technology for their support and helpful input; and to H. Jacqueline Brehmer for her research assistance.

Regulations or mandates imposed in one nation often have a ripple effect extending far beyond the nation's borders.

As a result, the debate often turns to the international—with both sides warning of the global side effects of the policies they oppose. The claims are varied, covering both the ways in which US regulation will have negative effects globally and the way in which the internationalization of digital communication networks will affect US regulatory efforts. Among the many concerns: If the United States demands access, repressive regimes will as well;[4] if the United States demands access, users will simply switch to non-US based providers, thus harming US businesses;[5] and if the United States demands access, the security of Internet users around the world will be undermined—and both users and governments worldwide will be exposed to an increased risk of malicious cyber attacks.[6]

Conversely, law enforcement and security officials deplore the international costs of doing nothing. The United States, after all, is home to the lion's share of communications providers. It has, as a result, regulatory jurisdiction over a significant majority of companies that control the world's data. If US-based companies are technologically unable to respond to lawful process, then they will effectively be exporting a security risk—the reduced ability to detect and respond to criminal activity—around the world.[7]

The purpose of this essay is to tease out these international effects arguments and their implications for the domestic regulatory process. What are the *specific,* potential international spillover effects of the *specific* regulations or orders being considered? How should these potential effects be substantively evaluated and weighed? What do they mean in terms of regulatory processes and goals that should be pursued?

My conclusion, perhaps unsurprisingly, is that these international effects matter. But they are incredibly difficult to evaluate. They depend, in significant part, on the degree and distribution of what I call the substitution effect—namely, the ease and willingness of consumers to substitute foreign-based products for US-based products subject to US regulatory and/or law enforcement jurisdiction and control. The degree and distribution of this substitution effect in turn depend, in part, on a range of factors that are largely outside of the US government's control, including foreign government policies and practices, product design of foreign-based providers, and consumer preferences, which are based in part on social trends. Put another way, the effects are bidirectional and dynamic. US policies and practices have a spillover effect internationally, but the policies and practices of foreign actors simultaneously

influence the effectiveness of any decryption and thus the scope and distribution of any US spillover effect.

This, of course, makes it difficult to evaluate, ex ante, the probable international spillover effects of any given policy or practice. But that is not to say they should be ignored. Rather, the international spillover effects are potentially significant, affecting both the effectiveness of any policy and the likely costs and benefits that will ensue. They should be monitored, assessed, and taken into account in the ongoing policy calculus, to the extent possible.

The remainder of this essay proceeds as follows: part 1 begins with a brief categorization of the decryption efforts being pursued; part 2 categorizes the international effects claims and explains how they map onto the different decryption efforts described in part 1; and part 3 evaluates the implications for the regulatory process. Even if new statutory decryption requirements are not adopted, decryption efforts continue nonetheless—in the form of court-ordered access and hacking efforts. The potential international spillover effects of these efforts should be evaluated and accounted for in policy design and practice.

1. The Decryption Mandates

It is uncontested that encryption hinders law enforcement's ability to access sought-after communications and other data that can be critical in the investigation of crime. It is also uncontested that encryption protects both individual users and governmental agencies from cybercriminals and other malicious attackers and facilitates the ability of individuals to keep personal information private. As a result, no one—even the law enforcement officials most concerned about the prospect of "going dark"—proposes a blanket ban on the use of encryption on personal devices or for personal communications. Rather, three main responses to default and end-to-end encryption are currently being considered: (1) a "front door" mandate requiring that providers maintain, as an element of product design, a way to access some or all devices, smartphone operating systems, and communications products; (2) ad hoc, compelled assistance that depends, in part, on the feasibility and burdensomeness of the sought-after assistance; and (3) a judicially sanctioned hacking regime. There is wide variation as to how each of these might be operationalized—and the specific details matter. But for the purpose of this discussion, I will group the ongoing decryption efforts into these three general buckets.

It is also important to note that while the "going dark" discussion is most often linked to the encryption debate, law enforcement's concerns are actually much broader. They

encompass end-to-end and default full disc encryption, but they also extend to other technological choices that limit governmental access, including use of anonymization tools and security defaults that erase a device after a certain number of incorrect password guesses.[8] This discussion covers the full array of technology-based efforts to provide law enforcement access to data in a readable form, including efforts to unlock devices—bundling all such efforts under the general heading of "decryption." The discussion thus encompasses efforts to access both data in motion and data at rest and operates at a relatively high level of generality. In practice, however, there are often nuanced legal, policy, and technological distinctions in terms of how these categories of data are treated and exploited.

A. Front Door Mandate

A front door mandate requires providers to maintain or develop a way to access encrypted communications in decipherable form in response to a lawfully obtained court order. There are several different forms such a mandate could take. One widely discussed proposal, put forward by Senators Richard Burr and Dianne Feinstein, the chair and vice chair of the Senate Select Committee on Intelligence, respectively, would require a wide range of Internet service providers (ISPs), device and software manufacturers, and other parties involved in the processing or storage of data to either turn over sought-after data in an "intelligible form" or provide the technical assistance to do so.[9] The requirement applies whether the information is sought by federal, state, or local officials, so long as it is pursuant to a court order and in the investigation of a range of specifically listed crimes.[10] Moreover, it applies in all situations that meet the specified criteria, without regard to the feasibility of compliance.[11] This, in effect, requires providers, manufacturers, and software developers to maintain, ex ante, a way to access their users' data—or risk running afoul of the law.[12]

Such an approach differs from what has often been described as a backdoor in that it is the companies—the providers and manufacturers—that maintain the decryption tools, not the government.[13] It does not require any *specific* product design; it just mandates that companies maintain *some* way to decode encrypted devices or data.

The initial Burr-Feinstein proposal represents a particularly broad front door mandate. Almost all the key elements—who is entitled to the decrypted data, who is subject to the mandate, and the scope of application—are far-reaching. There are other possible ways to design a front door mandate that would not be quite so expansive. For example, one could specify that only federal law enforcement officials are authorized to compel decryption, thereby maintaining national-level control as to when and under what circumstances companies were required to decrypt their users' data or unlock their

devices. One could also impose the decryption requirement on a smaller subset of companies, individuals, or products rather than the full range of companies involved in the processing or storage of data covered by the Burr-Feinstein draft bill. One option, for example, would require companies to maintain a way to unlock smartphones and other analogous devices, without also imposing an equivalent mandate with respect to communications in transit. Such a mandate would, for example, require Apple to maintain the means to access the stored data on a recovered iPhone, but it would not prohibit end-to-end encryption of iMessages.

The list of applicable crimes that would trigger a decryption mandate also can be narrowed or widened, thus decreasing or increasing the frequency by which the requirement would be imposed. That said, it is important to note that while any such narrowing will limit the situations in which the government could exercise the authority to compel, it would not change the key, de facto requirement that the provider either maintain or develop the technological capacity to decode its users' devices or data.[14] After all, the technology required to unlock a device or decrypt communications does not vary by crime.

B. Compelled, Ad Hoc Access

Even under the Burr-Feinstein draft bill, a court order is required; only when such an order is in place does the obligation to either decrypt or provide the requested technological assistance to do so kick in.

But independent judicial orders mandating decryption may be issued in the absence of a legislative mandate that providers maintain the means to provide access. This kind of ad hoc, ex post court order is what the US government initially—and very publicly—sought with respect to the iPhone recovered in the wake of the San Bernardino, California, shooting. Specifically, the government, relying on the All Writs Act, asked Apple to override the automatic lock feature that would have erased the phone's data after ten unsuccessful password attempts. While the government was ultimately able to unlock the iPhone with the assistance of a private company, and subsequently withdrew its request for compelled assistance future cases are likely to raise the same issues.[15] In fact, a federal prosecutor recently revealed that federal law enforcement has relied on the All Writs Act to compel Apple to unlock iPhones seventy times.[16]

One of the oldest federal statutes on the books, the All Writs Act gives courts residual authority to enforce their orders.[17] It does not provide the independent authority to compel. Rather, it serves as a supplemental authority in situations where the

government already has obtained a separate, independent order—such as a warrant compelling the production of sought-after data.

But a court's authority pursuant to the All Writs Act is limited. As interpreted by the Supreme Court and subsequent case law, application of the All Writs Act requires courts to consider at least three factors: first, whether the compelled assistance would impose "unreasonable burdens" on the company; second, whether it would be "consistent with the intent of Congress"; and third, whether the company's assistance is "necessary" to carry out the court's order.[18] While all three prongs were deeply contested by the parties, the question of burden is the most interesting one for the purpose of this essay. It considers the practicability and feasibility of compliance and, in the San Bernardino case, yielded a debate about the international effect of any exceptional access order. I return to these issues in part 2.

Newly adopted legislation in the United Kingdom provides an additional example of an ad hoc compelled assistance requirement. The UK legislation authorizes the secretary of state, subject to judicial approval, to require the provision of decryption assistance when "practicable" for the relevant operators to comply.[19] In determining what is practicable, the secretary of state must consider both the technological feasibility and the cost of compliance.[20] Reports indicate that Senators Burr and Feinstein are similarly considering revising their draft bill to make technical assistance subject to a "reasonable efforts" limitation thereby transforming their front-door mandate into an explicit statutory authorization of compelled, ad hoc access.[21] Unless these requirements are somehow interpreted to include an ex ante requirement that companies maintain the technological capacity to access their customers' data, one could easily imagine a company designing a system with no "practicable" or "reasonable" way in—thus avoiding the decryption mandate. Such compelled, ad hoc access is thus distinguished from a front door mandate, which either implicitly or explicitly requires providers to *maintain* the technological ability to access sought-after data.

C. Lawful Hacking

The third option—lawful hacking—is that which was ultimately employed in the San Bernardino case.[22] The government ultimately accessed the data with the help of a third party that discovered and exploited a vulnerability in Apple's code rather than forcing Apple to provide assistance. Such an approach has the advantage of protecting providers, manufacturers, and software developers from being forced to decrypt the very devices, operating systems, and communication platforms that they are working so hard to make secure. It thus relies on already-existing vulnerabilities,

rather than generating new ones. In the words of four prominent computer scientists who advocate a vulnerability-based approach to communications intercepts: "Instead of building wiretapping capabilities into communications infrastructure and applications, government wiretappers can behave like the bad guys. That is, they can exploit the rich supply of security vulnerabilities already existing in virtually every operating system and application to obtain access to communications of the targets of wiretap orders."[23]

But such an approach has disadvantages as well. It can be extraordinarily costly, making it an unrealistic option in run-of-the-mill cases. The San Bernardino exploit, for example, reportedly cost the federal government more than a million dollars.[24] It also relies on the unpredictable ability to exploit vulnerabilities, thus leading to situations in which sought-after data may not be available or decipherable in a sufficiently timely manner, even in those cases where the government is willing to devote the necessary resources to access the data. And it discourages the disclosure of known vulnerabilities.[25] If the exploitation of vulnerabilities is the only way in, law enforcement officials will be incentivized to hold onto their knowledge—and not disclose vulnerabilities—so that they can maintain a means of accessing sought-after data.

It is also worth emphasizing that a vulnerability-based approach is likely to be pursued even if a front door mandate is adopted or if courts widely order ad hoc access. No such front door mandates or court-ordered systems of ad hoc access are likely to be universal. As a result, there will continue to be situations in which the exploitation of vulnerabilities—otherwise known as "lawful hacking"—is the only or fastest way to access sought-after data.

2. International Spillover Effects

Debates about the various possible approaches to decryption (and each of the options discussed in part 1) are nuanced, heated, and ongoing. My purpose here is to focus on one narrow aspect of the debate: the claimed international spillover effects. While the anti-decryption proponents are often the most vocal in raising concerns about the international effects of attempted regulation, they are not the sole proprietors of such arguments. Law enforcement and security officials similarly invoke such claims when they warn of the international security consequences of *failing* to adopt new decryption requirements.

Specifically, I identify and assess five of the most oft-cited international spillover claims: (a) practical, (b) rights-based, (c) economic, (d) security-based, and (e) jurisdictional. In many cases, the international spillover claims are simply a

reprise of domestic arguments transposed onto the international stage. The competing security concerns are, for example, nearly identical whether one is talking about the security of domestic users or the security of foreign users. But other considerations—like the practical and rights-based concerns—raise normative and empirical considerations that stem from the global nature of the Internet and the global market in devices, software, and communication platforms. Moreover, whereas most of these claims relate to either a front door mandate or compelled, ad hoc access, a regime of lawful hacking also raises unique jurisdictional issues addressed below.

A. The Practical Considerations

A recent report identified 865 hardware and software products that incorporate encryption, of which two-thirds originated from outside the United States.[26] Another report found that eight out of nine encryption applications used by the Islamic State for secure communication are either foreign-based or open code (i.e., already in the public domain) and thus outside the scope of US regulatory jurisdiction or unlikely to be affected by such regulations.[27] Many argue that any US-imposed decryption mandate (either in the form of a front door mandate or compelled, ad hoc access) will be ineffective as a result.[28] Users can simply switch to other, foreign-based products and providers that are not subject to US jurisdiction or law.

Others, however, contest the thesis that users will switch products in order to maximize the security (encryption) of their data. As the scholar Herb Lin points out, most users appear to care more about performance, elegance, and convenience than the kind of security and privacy that encryption provides.[29] To be sure, these preferences change with a combination of technological developments and effective marketing, but—at least in the short term—the substitution effect probably won't be particularly widespread, according to this view. Yes, one million Brazilians reportedly signed up for Telegraph within hours of a Brazilian shutdown of WhatsApp in 2015[30]—but that was presumably because WhatsApp had been shut down completely. If WhatsApp had still been available, without end-to-end encryption but with its functionality intact, any such substitution effect would probably have been much reduced.

But even if Lin's analysis is right (which seems likely), it tells us about the behavior of the average user, not all users. Already, sophisticated cybercriminals, terrorists, and foreign adversaries are turning to secure technologies outside the regulatory jurisdiction of the United States. Such actors will probably pay attention to the US government's decryption efforts and continue to seek out—or develop—products that are outside the reach of the United States.

If correct, this means that a US-based decryption mandate (whether a front door mandate or compelled, ad hoc access) will be most effective in addressing the average consumer's use of encryption. Conversely, it will be significantly less effective in terms of limiting the use of encryption by sophisticated cybercriminals, terrorists, and other malicious actors who are much more likely to find ways to avoid any decryption regime. Put another way, it would facilitate local law enforcement access to data in the investigation of ordinary crimes, as well as in investigations of less sophisticated lone-wolf or homegrown terrorists. However, it may not be particularly useful in addressing law enforcement access concerns with respect to the more sophisticated, and arguably more dangerous, criminal and terrorist actors.

Importantly, any applicable substitution effect is also likely to vary by product. US-based companies, for example, produce over 95 percent of the operating systems for smartphones used worldwide—with Google's Android, Apple's iOS, and Windows Phone in the lead.[31] A decryption mandate as applied to these operating systems is, at least in the short term, likely to be highly effective—potentially even with respect to the more sophisticated actors—because there are relatively few substitutes available. By comparison, a decryption mandate as applied to specific communications apps may be significantly less effective. Foreign-based companies produce a wide range of communications platforms that are compatible with a range of operating systems.[32] Unless the government were to couple a decryption mandate with a prohibition on *use* of foreign-based applications that fail to comply with US regulatory requirements, users can still turn to foreign-based products, many of which employ end-to-end encryption. Such a use-based restriction seems improbable; it is hard to imagine that such a broad prohibition on the use of foreign-based communication tools, including some that the United States helped develop, would have sufficient political support to be enacted.

Of course, the probable substitution effects will be minimized if the United States acts in conjunction with other international partners, rather than simply acting alone. But, at least in the short term, the kind of widespread international cooperation needed to meaningfully limit the substitution effects is unlikely. The issues are simply too contested, and the range of perspectives too varied, to reach any kind of global (or near-global) response to the difficult policy questions posed by encryption. For the purposes of this essay, I thus assume the United States is acting alone.

Moreover, even if the international community were somehow able to reach a consensus as to the right approach and join forces in implementation, no such decryption mandate is likely to fully eliminate the kind of substitution effects discussed

here. After all, many encryption tools are open source. The most sophisticated (and malicious) actors will look for a way to communicate securely, even if they violate the law in doing so.

B. Human Rights Considerations

Dissidents and human rights activists around the world rely on end-to-end encryption and the security of their devices to communicate, network with other activists, and build political opposition movements in repressive states. The concerns are twofold.

First, if the United States imposes a decryption mandate, the software and devices that human rights activists and dissidents rely on to communicate will no longer be effective in providing adequate protection. This, however, is not the case if the substitution effect discussed above is strong and users can employ circumvention techniques to avoid any applicable restrictions on the use of encryption. Thus the strength of the human rights concern depends directly on the availability and feasibility of employing substitute technologies.

Second, and distinctly, many warn that any US-imposed mandate will either be mimicked by, or bolster the implementation of, already-existing mandates by other repressive regimes in ways that put human rights activists and dissidents at risk.[33] US-based providers and software developers can currently respond to decryption demands by asserting the technological impossibility of doing so. But they will no longer be able to make that claim if either US law imposes a front door mandate on such companies or ad hoc court cases require decryption—and that fact is known.

Apple made this precise argument in its briefing in the San Bernardino case. In claiming excessive burden, Apple warned that the government's sought-after order would "adversely affect Apple's interests and those of iPhone users *around the globe*."[34] Specifically, Apple argued that an order mandating it to develop a way to access the phone's data would threaten the security of its systems and thus hundreds of millions of customers—both domestic and foreign.[35] It also warned that the government's requested order would lead to increased pressure from foreign governments making demands for similar access.[36]

The government, for its part, disagreed that there would be any significant security risk to users, whether domestic or foreign. Moreover, it suggested that the risk of increased surveillance by foreign governments was not a legitimate factor for the court to consider. In the government's words: to the extent that the company faces

foreign pressure, that "flows from [Apple's] decision to do business in foreign countries, not from the Order."[37] In other words, if Apple were troubled by foreign government responses, it should pull out of those markets.[38] Such a response, however, does not address the broader normative concern about the security of foreign users.

More broadly, many warn that both the US government and US-based companies will find it increasingly difficult to argue against decryption mandates employed by repressive regimes if the United States is, at the same time, imposing its own decryption mandates. Some argue this is a specious concern—that foreign encryption laws are not likely to be affected by a US mandate.[39] After all, countries like China and Russia are likely to demand access no matter what the United States does or does not do. And in fact, on July 7, 2016, Russia adopted a new counterterrorism law that requires Internet companies to provide to security officials information "necessary for the authorities to achieve their statutory goals"—that is, information necessary to decode the electronic messages of interest to the government.[40]

But while certain countries will demand access irrespective of US policy, the existence of a US decryption mandate makes it harder for companies to resist both in specific individual cases and as a matter of policy. Moreover, while countries are not likely to follow in lockstep with US policy decisions in this area, it does seem probable that the many nations that are still working out a response to encryption will be emboldened—or persuaded —to adopt a decryption mandate that resembles, at least in part, US practices and policies. Thus, even if the *absence* of a US mandate does not dissuade countries set on mandating decryption from doing so, it is likely that the *existence* of a US mandate would, over time, have the effect of encouraging other nations to adopt and implement decryption regimes—and make it harder for US companies to resist orders to compel, even when issued by repressive regimes.

C. Economic Costs

The claim is that either a front door mandate or compelled, ad hoc access will reduce trust in both US-based providers and US-manufactured devices, thus incentivizing users to substitute foreign-based providers and/or purchase foreign-manufactured devices. A substitution effect—if widespread—could have significant effects on US companies, with a negative impact on the US economy as a whole. As described above, the validity of such concerns depends in large part on user preferences. If, as Lin has argued, users care more about other features of their devices and applications than about security and privacy, then the substitution effect may not be large; if, however, users increasingly value robust encryption, then these effects will likely grow over time.

Moreover, even if there is relatively little substitution among US users, past behavior suggests the likelihood of greater substitution among foreign users. The trust deficit that occurred after the Snowden revelations, for example, is reported to have cost US-based tech companies billions of dollars in lost contracts and sales, largely from foreign governments and businesses.[41] Assuming those estimates are accurate, they suggest that there is likely to be at least some substitution—and economic fallout—from regulation.

Moreover, it is worth noting that any substitution effect is likely to turn on the *perceptions* regarding the degree of governmental access, rather than the actual reality. The US debate about encryption already is, and is likely to continue to be, public, vociferous, and protracted. As long as the United States is *perceived* as mandating decryption, users may seek alternative providers and products that are both outside the reach of US regulatory jurisdiction and not subject to any US-based decryption mandate.[42] It also may not matter if other nations also support various forms of mandatory decryption, so long as the spotlight is on US-based surveillance. This means that even a relatively rare exercise of the authority to demand decryption could, if given extensive media and public attention, yield a strong substitution effect. And thus it could have a significant economic effect as well.

D. Security Concerns

This is the same security vs. security debate that applies domestically, yet transposed onto the international arena. Opponents of a decryption mandate warn of the risks of exposure of users' secure personal and sensitive data and their increased vulnerability to cybercriminals. If the United States imposes a decryption mandate, users of US products will be less secure—worldwide. I call this the "security risk" of decryption requirements.

The degree of this security risk varies by design. A front door mandate creates greater security risks than a situation in which courts order decryption on an ad hoc and relatively infrequent basis. Lawful hacking regimes also impose potential security costs; to the extent that such a regime discourages the disclosure of vulnerabilities, then such vulnerabilities remain available to malicious actors as well.

Conversely, proponents of such mandates warn of the costs to international security that could result from the inability to access information. From this perspective, a decryption mandate carries what I call a "security benefit"—one that, like the risk, is exported worldwide.[43] Just as the risk increases as the scope of the mandate expands,

so too does the benefit. A front door mandate provides the greatest benefit: a lawful hacking regime, the least international benefits, unless also coupled with information-sharing regimes.

That said, as already discussed, even a broad front door mandate is not likely to have the same security cost or benefit across different types of products and categories of users. As already stated, substitution is much easier with respect to communication apps than operating systems for smartphones and other devices. Moreover, sophisticated terrorists, cybercriminals, and foreign adversaries are much more likely to seek out tools that allow them to communicate securely, whereas more "ordinary" consumers may not realize that their data are subject to potential governmental access. And they may not be willing or knowledgeable enough to take the extra steps to employ more sophisticated encryption tools.

If this analysis is correct, it means that both the security risks and benefits will be concentrated on the ordinary user. Meanwhile, the more sophisticated terrorists, cybercriminals, and foreign adversaries will be better able to evade regulation. Governmental officials will continue to need to find alternative means of accessing their communications and devices—if at all.

E. Jurisdictional Issues

There are two sets of jurisdictional issues to consider. First are the jurisdictional limits of any proposed action. Obviously, a mandate will only be effective to the extent it is accompanied by enforcement authority over either the provider or the user—and such enforcement authority is actually exercised. The United States has no control over a foreign-based provider that lacks a presence in the United States. Nor does it have any direct control over a foreign-based user of such tools. This is an obvious point—and not at all unique to the issue of encryption. It is simply worth noting this reality, as it limits the scope of any potential mandate. A US decryption mandate would not have any impact on the ability of the government to access the communications of two Islamic State operatives in Syria who are using a foreign-based app like Telegraph to communicate.

Second, interesting jurisdictional questions arise pursuant to the lawful hacking approach to decryption—issues that have also been raised by the separate, but related, debate over recent amendments to Rule 41 of the Federal Rules of Criminal Procedure. Under the former federal rule, magistrate judges generally can issue warrants for searches conducted within their territorial jurisdiction only.[44] Some magistrates have, as a result, denied search warrants for devices of unknown whereabouts; if

the device is of an unknown location, it may be outside the judge's jurisdiction.[45] But this creates obvious problems for law enforcement, particularly given the rising use of anonymization tools as a means of concealing location. A pending change to Rule 41 addresses this problem. It explicitly allows magistrates to issue warrants for electronically stored media and data in those cases where the location of the media or data has been concealed through technological means.[46]

This, however, raises the prospect that judges may be authorizing searches or seizures of data that are located extraterritorially. Data on TOR users, for example, suggest that approximately 80 percent of such users are foreign-based—indicating that this is not just a possibility but a likelihood.[47] Such an extraterritorial search risks being perceived as a violation of the other nation's sovereignty and perhaps criminal laws.[48] When, for example, US agents investigating a Russian-based computer hacker remotely accessed his Russian computer, Russia filed criminal charges against the agents involved.[49]

3. The Assessment

The international spillover effects are varied, bidirectional, and dynamic. They depend to a significant degree on the scale and distribution of the substitution effect. This in turn will vary based on the particular regulation being put in place, its implementation and enforcement, its interaction with the regulations (or lack thereof) of foreign partners, and the reaction of users both domestically and internationally. These are in many cases known unknowns.

One possible response is to hold off on new regulations unless and until we can reach international consensus with enough of the world's key players to think that any particular mandate will be effective and thus any substitution effect stemmed.[50] But as already discussed, the diversity of international opinion means that international consensus is not something that will be achieved any time soon.[51]

Others take the position that we simply can't wait for the international community to come together or for the many uncertainties to be resolved—as this may never happen, or at least not in a sufficiently timely manner. That, after all, is the clear position of Senators Feinstein and Burr. But this barrel-on-forward approach is risky. While regulation often takes place in the face of uncertainty, the potentially large economic and security costs strongly suggest the need for caution here. And while the economic and security costs will decrease as the substitution effect increases, a significant substitution effect also means that the potential security *benefit,* from the perspective of law enforcement, will decrease as well.

Ultimately, whatever one thinks of the merits, the political realities make a front door legislative mandate hard to push through even a one-party controlled Congress. The debate is simply too polarized and too vociferous to reach the kind of consensus needed to pass new legislation on this issue at least in the short term.[52] Importantly, however, this is not the same as a "no decryption" policy. To the contrary, decryption efforts continue. Law enforcement officials will continue to pursue court-ordered, compelled assistance in unlocking phones or decrypting data, pursuant to the All Writs Act. Law enforcement agencies also will continue to seek to exploit vulnerabilities as a means of accessing sought-after data—either on their own or with the assistance of private parties. These ongoing efforts make courts and law enforcement agents the frontline actors in generating and responding to international spillover effects. The following sections address a few key implications of this reality.

A. The Courts

Courts increasingly are being put on the front lines of deciding encryption policy. Yet courts are not institutionally well equipped to evaluate the kind of international spillover effects discussed in part 2. Not only are the scope and distribution of any likely spillover effect difficult to determine, but they also depend, at least in part, on how often compelled access is sought and granted. Yet when a judge issues an order in particular cases, he or she has little way to know whether and how the order and underlying reasoning will be relied on, expanded, or curtailed in future cases. There is thus no way for the judge to know whether a single decryption order will mark the beginning of a large-scale, albeit court-ordered, decryption mandate or will operate as a one-off order relegated to the specific facts at hand.

Even if these factors were known, such broad-reaching policy considerations—particularly those that consider the impact on *foreign* users—are arguably irrelevant to the specific case or controversy before the court. In fact, the one international spillover effect that seems most appropriate for courts to assess is the one that has received the most ridicule from commentators: the business effect on the particular party that is before the court. While any claimed economic burden may ultimately be too speculative to be cognizable, these kinds of specific harms, relevant to the specific parties before the court, are at least the *kinds* of factors that courts ought to consider. By comparison, the broader policy implications as to how such an order will affect international security and the human rights of foreign users are undoubtedly important questions, but better addressed to the political branches than the courts.

It is thus the responsibility of the executive branch to take into account the potential international spillover effects in deciding whether and in what cases to pursue such decryption orders. While the executive is also operating in a world of uncertainty, and often subject to competing policy goals, it is at least better positioned than the courts to both assess and monitor the broader implications of a particular case. This suggests the need for a centralized approval process. Federal prosecutors should be required to get advance approval from the Department of Justice before seeking such orders. Department of Justice approval should depend on a full assessment of the potential security, rights-based, economic, and diplomatic implications of any sought-after orders. Moreover, the international spillover effects of any such orders (or lack thereof) should be monitored and learned from. This in time may ultimately provide the strongest fodder yet for new statutory regulations, perhaps as a means of reining in the executive and the courts or perhaps in an effort to give them greater authority to compel.

B. Lawful Hacking Regime

Unlike both a front door mandate and court-ordered access, lawful hacking is not likely to yield much, if any, in the way of substitution effects. After all, hacking can be used to access US-based and foreign-based products and communication systems alike. But they carry consequences that extend beyond our borders in two key areas: first, with respect to security; and second, with respect to the jurisdictional and sovereignty-based interests of foreign nations.

The security concerns have already been touched on: a lawful hacking regime depends on the exploitation of existing vulnerabilities. This has the advantage of relying on existing security weaknesses, rather than the generation of new ones. Yet it also discourages the disclosure of these vulnerabilities, as the disclosure means loss of law enforcement access. The continued existence of discovered vulnerabilities contributes to an all-around less secure environment; vulnerabilities can then be exploited by the good guys (law enforcement agents) and bad guys (malicious actors) alike. Moreover, certain kinds of network investigative techniques can introduce their own vulnerabilities. These security risks transcend national boundaries.

This suggests the need for executive branch control and clear-cut policies as to when the use of potentially intrusive network investigative techniques is permitted, and when and in what circumstances vulnerabilities should be disclosed. The decision to pursue such tools should, like the decision to invoke the All Writs Act to compel provider assistance, be centralized and coordinated within the Department of Justice. In general, lawful hacking should be turned to only when other less intrusive means

of accessing sought-after information are unavailable. Moreover, it is critical that the vulnerabilities equity process—by which government officials determine whether and when to disclose vulnerabilities—takes into account the full range of security trade-offs. The standards and processes employed should be a matter of public knowledge, and the process itself should be subject to increased congressional oversight.[53]

A lawful hacking regime also yields tricky jurisdictional and sovereignty-related issues resulting from law enforcement efforts to access data or devices that are located outside US territorial jurisdiction. Foreign governments are likely to object to what they perceive as extraterritorial hacking—just as the United States would and should object if and when foreign governments unilaterally access US-held data. These concerns further underscore the need for centralized, federal-level decision-making and clear procedures and policies for handling such situations. Among the many considerations: in what circumstances should such hacking efforts be pursued; whether and how to notify the host country; and whether, in what set of circumstances, and how quickly to cease any ongoing exploitation efforts. At a minimum, there ought to be federal-level control and clear guidelines about how to handle such situations.

This also may be one area where bilateral or multilateral agreement may be possible. After all, such cross-border accessing of data, particularly in the exploitation of devices or communications of unknown location, is almost certain to take place—instigated not just by the United States but by foreign partners as well. The US thus has a role to play—and will itself benefit from—mutually agreed-upon norms and practices; this is something that should be further explored.

Conclusion

Our digital networks are both global and territorial—increasingly subject to sovereign control. This reality has implications for policies and practices with respect to encryption as well as to a host of other efforts to regulate global digital communication networks. It means that our domestic regulations have international spillover effects, and it means that international policies, practices, and technological developments affect our ability to effectively regulate such networks. This essay attempts to tease out and analyze these effects. It does not provide the answers. There are simply too many known unknowns to do so. But it does take the position that these international effects matter—in both directions. They matter to the effectiveness of our regulatory efforts, and they matter in the ways they affect foreign actors, businesses, and governments.

It is also a mistake to think that the absence of new regulation signifies the absence of international effect. To the contrary, the absence of new regulation is itself a policy.

So are the ongoing efforts to seek court-ordered compelled access and the use of lawful hacking techniques as a means of accessing sought-after data. We should make sure that the potential international effects of these efforts are monitored and taken into account in determining whether or not to pursue decryption efforts. We should mandate centralized review and approval of federal prosecutors' decisions to seek court-ordered decryption assistance. We should develop clearer and more transparent rules and procedures regarding the disclosure of vulnerabilities. We should work with key allies to address those situations in which our law enforcement agents access devices of data outside our borders, and we should learn from these efforts and their effects.

NOTES

1 See, e.g., Bruce Schneier, "A 'Key' for Encryption, Even for Good Reasons, Weakens Security," *New York Times,* July 15, 2016, www.nytimes.com/roomfordebate/2016/02/23/has-encryption-gone-too-far/a-key-for-encryption-even-for-good-reasons-weakens-security; Ellen Nakashima, "Former National Security Officials Urge Government to Embrace Rise of Encryption," *Washington Post,* December 15, 2015, www.washingtonpost.com/world/national-security/former-national-security-officials-urge-government-to-embrace-rise-of-encryption/2015/12/15/3164eae6-a27d-11e5-9c4e-be37f66848bb_story.html; "UN: Online Anonymity, Encryption Protect Rights," Human Rights Watch, June 17, 2015, www.hrw.org/news/2015/06/17/un-online-anonymity-encryption-protect-rights; Kevin Bankston, "It's Time to End the 'Debate' on Encryption," *Just Security,* July 7, 2015, www.justsecurity.org/24483/end-debate-encryption-backdoors/.

2 See, e.g., Patrick Howell O'Neill, "FBI Director: 'There Is No Such Thing as Absolute Privacy in America,'" *The Daily Dot,* August 31, 2016, www.dailydot.com/layer8/comey-crypto-war-business-model/; James Comey, "Encryption, Public Safety, and 'Going Dark,'" *Lawfare* (blog), July 6, 2015, www.lawfareblog.com/encryption-public-safety-and-going-dark; see also Melissa Boughton, "Locked Phones Can Hinder Local Crime-Solving Efforts," *The Post & Courier,* March 6, 2016, www.postandcourier.com/article/20160229/PC16/160229296/1177/local-law-enforcement-access-to-encrypted-data-not-just-the-fbi-vs-apple.

3 See Cody M. Poplin, "FBI Director Comey's Remarks as Delivered," *Lawfare* (blog), October 16, 2014 (quoting James Comey: "[T]he notion that the marketplace could create something that would prevent that closet from ever being opened, even with a properly obtained court order, makes no sense to me"), www.lawfareblog.com/fbi-director-comeys-remarks-delivered.

4 See, e.g., Brief of Amici Curiae, Privacy International and Human Rights Watch, "In re the Search of an Apple iPhone Seized during the Execution of a Search Warrant on a Black Lexus IS300, No. 16-CM-10" (C.D. Cal. March 3, 2016), 12–21; "Don't Panic: Making Progress in the 'Going Dark' Debate," Berkman Center for Internet & Society, Harvard Law School, February 1, 2016, 9 (noting that "if the U.S. government were to mandate architectural changes, surveillance would be made easier for both the U.S. government and foreign governments, including autocratic regimes known to crack down on political dissidents"), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

5 See, e.g., "Going Dark, Going Forward: A Primer on the Encryption Debate," House Homeland Security Committee Majority Staff Report, June 2016, 18 (raising the possibility that "U.S. legislation might have little impact on bad actors that can obtain encryption tools outside of the United States, while irreparably harming U.S. commercial interests by driving customers to foreign competitors"); Bruce Schneier, Kathleen

Seidel, and Saranya Vijayakumar, "A Worldwide Survey of Encryption Products," February 11, 2016, 6–7, www.schneier.com/cryptography/paperfiles/worldwide-survey-of-encryption-products.pdf.

6 See, e.g., Apple's motion to vacate, "In re the Search of an Apple iPhone Seized during the Execution of a Search Warrant on a Black Lexus IS300, No. 16-CM-10" (C.D. Cal. February 25, 2016), 23 (emphasizing that its "data protection systems . . . ensure the security of hundreds of millions of customers" and that "[a]n order compelling Apple to create software that defeats those safeguards . . . adversely affects [the interests of] iPhone users around the globe").

7 See, e.g., James B. Comey, "Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy," Joint Statement with Deputy Attorney General Sally Quillian Yates before the Senate Judiciary Committee, Washington, DC, July 8, 2015 (warning of the global "public safety risks if criminals can plan and undertake illegal acts without fear of detection"), www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy.

8 Another relevant factor is the trend toward data localization that results in sought-after data being moved beyond the reach of US law enforcement. This problem has been significantly exacerbated by the Second Circuit decision in the Microsoft Ireland case, which, with respect to stored communications content, limits the reach of the US warrant's authority for stored communications content to data that are held within the territorial borders of the United States. See "In re Matter of a Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft," 829 F.3d 197 (2d Cir. 2016); Jennifer Daskal, "The Dangerous Implications of the Microsoft Ireland Case," *Just Security,* October 14, 2016, www.justsecurity.org/33577/dangerous-implications-microsoft-ireland-case/. This issue, however, falls beyond the scope of what I am addressing here.

9 Richard Burr and Dianne Feinstein, Compliance with Court Orders Act of 2016, § 3(a)(1), April 13, 2016 (discussion draft), § 3(a)(1), www.burr.senate.gov/imo/media/doc/BAG16460.pdf. Reports indicate that the senators may be considering revisions to this proposal. See, e.g., Julian Sanchez, "Feinstein-Burr 2.0: The Crypto Backdoor Bill Lives On," *Just Security,* September 9, 2016, www.justsecurity.org/32818/feinstein-burr-2-0-crypto-backdoor-bill-lives/.

10 Burr-Feinstein, Compliance with Court Orders Act, §§ 4(3), (8).

11 That said, reports indicate that the senators are considering revisions that would add in a "reasonable efforts" limitation on the requirement of technical assistance, and thus operate more like an ad-hoc, compelled access type of mandate. See Sanchez, "Feinstein-Burr 2.0."

12 The legislation does not include any specific penalty for noncompliance. Burr indicated this was a decision best left to individual judges. See Julian Hattem, "Intel Chair: Encryption Bill Won't Specify Noncompliance Penalties," *The Hill,* April 12, 2016, http://thehill.com/policy/cybersecurity/275993-intel-chairman-judge-will-decide-penalties-under-encryption-bill.

13 I do not include a separate discussion of such "backdoor" mandates, given that even advocates of a strong government-mandated decryption regime are not currently pushing such an approach. For a good analysis of the associated security risks, see Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore et al, "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," Massachusetts Institute of Technology, Computer Science and Artificial Intelligence Laboratory Technical Report, July 6, 2015, http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8.

14 It is, of course, possible that the list of applicable crimes is so narrowed that companies could reasonably presume that they would not be subject to such a mandate. But that would be an insufficient mandate from the perspective of law enforcement; after all, those pushing decryption mandates assert that they are being stymied in their investigations in a wide range of cases.

15 See Katie Benner and Eric Lichtblau, "U.S. Says It Has Unlocked iPhone without Apple," *New York Times,* March 28, 2016, www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html.

16 See Lorenzo Franceschi-Bicchierai, "Fed Says Apple Has Unlocked Suspects' iPhones 'At Least' 70 Times in the Past," *Motherboard,* October 26, 2015, http://motherboard.vice.com/read/feds-say-apple-has-unlocked-suspects-iphones-at-least-70-times-in-the-past. See also Eliza Sweren-Becker, "This Map Shows How the Apple-FBI Fight Was about Much More Than One Phone," American Civil Liberties Union, March 30, 2016, www.aclu.org/blog/speak-freely/map-shows-how-apple-fbi-fight-was-about-much-more-one-phone. That said, these prior cases were in key respects less controversial. They all appear to have been directed at phones using older operating systems, pursuant to which Apple (or other companies to whom the requests were directed) maintained encryption keys for its devices, thus enabling relatively easy compliance with the court order. Yet even orders of assistance with respect to this earlier technology have been successfully challenged. See "In re Order Requiring Apple to Assist in the Execution of a Search Warrant Issued by This Court, 149 F.Supp.3d 341" (E.D.N.Y. 2016). For phones running on its newest operating systems, Apple no longer maintains the encryption keys; the phones are also designed to automatically lock and delete after ten missed password attempts, making it impossible for the government to try to access through a brute force attack (in the form of repeated password attempts). In the San Bernardino case, therefore, the government sought a different kind of assistance than it had requested before: it effectively asked Apple to override an existing security feature and write new code to do so.

17 28 U.S.C. § 1651(a) (1949) (giving federal courts the authority to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law").

18 See United States v. New York Tel. Co., 434 U.S. 159, 172 (1977).

19 Investigatory Powers Act 2016 c. 25 (Eng.), § 253 (4), http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf.

20 Ibid. § 255 (3)–(4).

21 See Sanchez, "Feinstein-Burr 2.0."

22 I use the term "lawful hacking" broadly to cover communication intercepts, remote searches, and the accessing of devices that are already in the government's possession (as in the San Bernardino case). There are, however, important technological distinctions in how these different efforts are operationalized and thus the legal and policy issues that ensue; remote searches, for example, raise jurisdictional issues (discussed below) that are simply irrelevant to governmental efforts to access a device in their possession.

23 See Steven Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, "Lawful Hacking: Existing Vulnerabilities for Wiretapping on the Internet," *Northwestern Journal of Technology and Intellectual Property* 12, no. 1 (2014): 5.

24 See, e.g., Wesley Bruer, "FBI Paid More Than $1 Million to Hack San Bernardino Shooter's iPhone, Comey Says," CNN, April 21, 2016, www.cnn.com/2016/04/21/politics/san-bernardino-iphone-apple-hacking/.

25 See, e.g., Ari Schwartz and Rob Knake, "Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process," The Cyber Security Project, Belfer Center for Science and International Affairs, June 2016, 8, http://belfercenter.ksg.harvard.edu/files/Vulnerability%20Disclosure%20Web-Final4.pdf.

26 Schneier et al., "Worldwide Survey."

27 Kevin Bankston, Ross Schulman, and Jake Laperruque, "The Crypto Cat Is out of the Bag: An Illustrative Inventory of Widely-Available Encryption Applications," New America's Open Technology Institute,

December 8, 2015: 1, https://static.newamerica.org/attachments/12155-the-crypto-cat-is-out-of-the-bag/Crypto_Cat_Jan.0bea192f15424c9fa4859f78f1ad6b12.pdf.

28 See, e.g., Schneier et al., "Worldwide Survey," 6–7; Bankston et al., "Crypto Cat," 1–2; *Deciphering the Debate over Encryption: Industry and Law Enforcement Perspectives: Hearing before H.R. Subcommittee. on Oversight & Investigations, Committee on Energy and Commerce,* 11th Cong. 57 (2016) (statement of Rep. Morgan Griffith), ("[I]f we force the companies that we do have jurisdiction over to weaken the security of their products, are we doing little more than hurting American industry and then sending the really bad actors like Mr. Fletcher, who is the child pornographer, just to a different format that we don't have control over?") http://docs.house.gov/meetings/IF/IF02/20160419/104812/HHRG-114-IF02-Transcript-20160419.pdf.

29 See Herb Lin, "Brennan's Recent Testimony on Encryption," *Lawfare* (blog), June 22, 2016, www.lawfareblog.com/brennans-recent-testimony-encryption.

30 See Mike Murphy, "Brazil Shut down Whatsapp for Roughly 100 Million People for 12 Hours," *Quartz,* December 17, 2015, http://qz.com/576485/brazil-has-shut-down- whatsapp-for-roughly-100-million-people/.

31 Smartphone OS Market Share, 2015 Q2, International Data Corporation, www.idc.com/prodserv/smartphone-os-market-share.jsp.

32 Schneier et al., "Worldwide Survey," 2–5.

33 See, e.g., Brief of Amici Curiae, Privacy International and Human Rights Watch, 19–21.

34 Apple motion to vacate, 23 (emphasis added).

35 Ibid.

36 Ibid., 24.

37 Government reply in support of motion to compel, "In re the Search of an Apple Iphone Seized during the Execution of a Search Warrant on a Black Lexus, No. 16-CM-10" (C.D. Cal. Mar. 10, 2016), 26.

38 Ibid., 26–27 (recasting the claimed burden as an "inevitable consequence of Apple's own business decisions").

39 See Jack Goldsmith, "Encryption and Territorial Regulation" (forthcoming 2016), (manuscript on file with author).

40 See Ksenia Koroleva, "'Yarovaya Law'—New Data Retention Obligations for Telecom Providers and Arrangers in Russia," *Global Privacy & Security Compliance Law* (blog), Latham & Watkins, July 29, 2016, www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/; "Russia: 'Big Brother' Law Harms Security, Rights," *Human Rights Watch,* July 12, 2016, www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights. The law will go into effect on July 1, 2018.

41 See Robyn Greene, Danielle Kehl, Robert Morgus, and Kevin Bankston, "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity," New America's Open Technology Institute. July 29, 2014, 7–11 (summarizing various reports of lost revenue), www.newamerica.org/oti/policy-papers/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/; Elizabeth Dwoskin, "New Report: Snowden Revelations Hurt U.S. Companies," *Wall Street Journal,* July 30, 2014, http://blogs.wsj.com/digits/2014/07/30/new-report-snowden-revelations-hurt-u-s-.

42 In that regard, Apple's vociferous opposition to the sought-after order in the San Bernardino case was arguably contrary to its own interests (or, cynically, strengthened its argument to the court); quiet acquiescence might limit the substitution effect, and thus the economic burden, of such a mandate.

43 Proponents of such mandates also challenge the idea that carefully controlled access will in fact yield a security risk—or at least enough of a security risk to preclude regulation. See, e.g., O'Neill, "No Absolute Privacy" (citing James Comey: It is "a false premise to say that the only answer to the challenge we face is to introduce vulnerabilities into code").

44 See Federal Rules of Criminal Procedure, 41(b) (listing the sole instance in which out-of-district search warrants are permitted).

45 See "In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 761" (S.D. Tex. 2013).

46 See proposed amendment to Rule 41, Advisory Committee on Rules of Criminal Procedure, April 2014, 165–66, www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda Books/Criminal/CR2014-04.pdf.

47 "Top-10 Countries by Directly Connecting Users," Tor Project, https://metrics.torproject.org/userstats-relay-table.html.

48 See Jennifer Daskal, "The Un-Territoriality of Data," *Yale Law Journal* 125 (2016): 325, 326–38; Richard Salgado, Google Inc., "Comments on the Proposed Amendment to Federal Rules of Criminal Procedure 41" (2015), 3–4 (warning of the potential sovereignty-related concerns that would arise if US law enforcement agents were to search devices located in other nations), www.regulations.gov/#!documentDetail;D=USC-RULES-CR-2014-0004-0029.

49 See Mike Brunker, "FBI Agent Charged with Hacking," MSNBC, August 15, 2002, www.nbcnews.com/id/3078784/#.VM178lph3L9; United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, (W.D. Wash. May 23, 2001), 1.

50 See, e.g., Anne Johnson, Emily Grumbling, and Jon Eisenberg, rapporteurs, *Exploring Encryption and Potential Mechanisms for Authorized Government Access to Plaintext: Proceedings of a Workshop* (Washington, DC: National Academies Press, 2016), 9, http://cryptome.org/2016/08/nap-encryption-gov-access.pdf; ibid., 43 (describing both Chris Inglis, a 28-year veteran of the NSA, and James Baker, the general counsel of the FBI, as taking the position that "some form of international coordination . . . is necessary to make [exceptional access mandates] even remotely effective").

51 See House Homeland Security Committee, "Going Dark, Going Forward," 13–15 (summarizing different countries' approaches to encryption).

52 See, e.g., Sara Sorcher and Joshua Eaton, "What the US Government Really Thinks about Encryption," *Christian Science Monitor,* May 25, 2016, www.csmonitor.com/World/Passcode/2016/0525/What-the-US-government-really-thinks-about-encryption; Joseph Menn and Dustin Volz, "Apple Case Exposes Ongoing Government Rift over Encryption Policy," Reuters, March 7, 2016, www.reuters.com/article/us-apple-encryption-schism-insight-idUSKCN0W70U5.

53 For a particularly thoughtful set of recommendations with respect to lawful hacking, see Susan Hennessey, "Lawful Hacking and the Case for a Strategic Approach to Going Dark," Brookings Institution, October 7, 2016, www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/. See also Bellovin et al., "Lawful Hacking," 58–62; Schwartz and Knake, "Government's Role," 12–18 (recommending a series of improvements to the vulnerability equities process).

About the Author

JENNIFER DASKAL

Jennifer Daskal is an associate professor of law at American University's Washington College of Law, currently on leave while working as an Open Society Institute Fellow on issues related to privacy and the cross-border flow of data. From 2009–2011, Daskal was counsel to the assistant attorney general for national security at the Department of Justice.

Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cyber security, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The working group's output, which includes the Aegis Paper Series, is also published on the *Lawfare* blog channel, "Aegis: Security Policy in Depth," in partnership with the Hoover Institution.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200