A HOOVER INSTITUTION ESSAY

Decryption Mandates and Global Internet Freedom

TOWARD A PRAGMATIC APPROACH

ADAM I. KLEIN

Aegis Paper Series No. 1608

The debate over law enforcement and widespread strong encryption implicates powerful competing values. On one side, the liberty, privacy, and cybersecurity of American consumers and companies; on the other, the need to investigate serious crimes and protect the country against terrorism. Should companies be compelled to weaken their products (as most technologists see it)? Does the Fourth Amendment's "balance" require that law enforcement retain the ability to access data covered by a search warrant?[1] Does law enforcement really need such a mandate to investigate effectively?[2] Does the First Amendment permit Congress to enact a ban on encoding one's communications? Would such a ban be effective given the proliferation of new, powerful, easily accessible encryption technologies, including many created by foreign companies?

These are weighty questions, but they are analogous to the difficult trade-offs posed by many other debates over domestic counterterrorism measures since 9/11. What arguably distinguishes the encryption debate from earlier struggles over national security and civil liberties is the degree to which the potential *international* reverberations have been a significant and contested factor. Opponents contend that if the US government imposes a decryption mandate, authoritarian regimes will follow suit, and will use that access to oppress dissidents and cement their hold on power. They also argue that government efforts to undermine anonymization and encryption contradict the US government's own Internet-freedom agenda, a policy goal touted by senior officials in successive administrations and backed by tens of millions of dollars in government funding.

Unfortunately, like other aspects of the encryption controversy, the policy debate over encryption's international implications has been conducted principally in ideological terms rather than on the basis of observable facts and fact-based predictions about future developments.[3] This paper does not attempt to resolve either the ideological or factual disputes surrounding the international implications of US encryption policy. Rather, it proposes key questions to stimulate and guide a more factually informed debate about the international human-rights consequences of domestic encryption policy. And it contends

Adam I. Klein is an international affairs fellow at the Council on Foreign Relations and a visiting fellow at the Center for a New American Security.

that the parties will be more effective at persuading uncommitted observers—including members of Congress—if their arguments are pragmatic and factually supported rather than purely ideological. It concludes by offering a few modest recommendations for shifting the debate over the international aspects of encryption policy onto sounder empirical terrain.

The Policy Landscape: National Interests, Transnational Technology

The struggle over the international implications of the encryption debate exemplifies tensions inherent in many policy debates over national security, technology, and privacy. The difficulty arises from the fact that the US government must simultaneously practice interest-driven great-power politics, which includes conducting espionage; enforce the domestic laws of the United States; wage an unrelenting campaign to prevent terrorist attacks—which often requires cross-border cooperation and information sharing; promote rule-of-law norms, civil-society development, and democratic movements in illiberal states; and protect the commercial interests of US companies doing business overseas.

These various policy imperatives frequently pull in directions that are damaging to the others. The subject of this paper—the clash in the encryption debate between effective law enforcement and support for dissident movements—is, arguably, a prime illustration. That said, it is too simplistic to reduce the discussion over the international aspects of tech-privacy debates, including that over encryption, to a straightforward clash between American security and American values. Even seemingly aligned imperatives can clash in ways that are less obvious.

One example is the tension between strategic intelligence and counterterrorism. Effective counterterrorism requires seamless cooperation between allied governments. This may include sharing personally identifiable information about one another's nationals—but aggressive signals- and human-intelligence targeting of foreign governments, if revealed, can undermine foreign publics' willingness to tolerate such sharing. The 2013 revelation that the United States was monitoring a personal cell phone used by German Chancellor Angela Merkel triggered a massive public backlash in Germany.[4] Subsequent reports that the United States had recruited human agents within the German government exacerbated the rupture, to the point that Germany expelled the CIA chief of station in Berlin.[5] The coup de grâce came when a German parliamentary committee discovered that, as part of a joint operation, the National Security Agency (NSA) had surreptitiously fed the *Bundesnachrichtendienst* (BND), German's foreign-intelligence agency, "selectors" that targeted European institutions and governments.[6] This led to a severe, albeit temporary, rupture in US-German relations, intense scrutiny of the BND's joint ventures with the NSA, and draft legislation regulating such SIGINT (signals intelligence) cooperation.[7]

It has taken three years for the bilateral relationship to recover from these once-unimaginable depths, to the point where German officials are again willing to publicly

tout counterterrorism cooperation with the United States.[8] All of which is to say that the familiar dialectic pitting national security against privacy fails to account for the many ways in which decisions involving technology, privacy, and national security may force policymakers to choose *among* national-security goals.

More relevant for present purposes is that these tech-policy choices can also pit one values-based goal against another. For example, as discussed in greater detail below, encryption and anonymization tools have been a significant element of the US government's efforts to support dissident movements in authoritarian countries—an expression and practical demonstration of American values. Yet strong encryption simultaneously can obstruct another largely values-based commitment in US foreign policy: assisting allies in their efforts to detect and disrupt terrorist plots. After the Paris attacks, President Obama "surged" counterterrorism assistance to Western European allies, particularly the overwhelmed Belgian security services.[9] Unfortunately, the Brussels attacks and their chaotic aftermath only illustrate how badly European allies need such US support.[10] Yet it appears that end-to-end encryption is increasingly frustrating these efforts. A recent *ProPublica* article describes frantic joint efforts in the aftermath of the Paris attacks to find the remaining plotters before they struck again:

> European spy agencies and their allies in the United States and Britain deployed the full weight of their sophisticated technology in the search for the plotters. But neither the NSA nor Britain's Government Communications Headquarters (GCHQ), spotted the digital footprints, officials said.
>
> "Everyone was trying to find these guys," the senior French counterterror official said. "They were able to elude us. But they were able to elude the Americans, too, and that shows you what a problem encryption is."[11]

Even human-rights concerns do not necessarily all cluster on one side of the debate. A central focus of international child-pornography investigations is, naturally, identifying the children depicted in the images and ending their suffering by arresting their abusers. Encryption makes it more difficult for law enforcement to identify victims, for the simple reason that perpetrators can deny police access to their stored images by deploying sophisticated disk encryption.[12] Meanwhile, anonymizing tools like Tor make it much more difficult for police to identify and hold accountable those who distribute images of child exploitation online.[13] To some extent, the interests of these children, whose abusers exploit anonymity on the Internet, clash with those of dissidents, activists, minorities, and journalists in authoritarian countries, who are protected by it.

This paper, however, focuses on one specific aspect of the encryption debate: the challenge of reconciling the US government's interest in accessing the contents of some encrypted data with its aspiration to support dissident movements and individual freedom in

authoritarian countries. Tension between pragmatism and idealism has been a leitmotif of American foreign policy since the early years of the republic. What differentiates current policy challenges at the nexus of security, technology, and privacy, however, is that even *domestic* policy choices reverberate immediately and often forcefully in the international arena. What's more, these effects are foreseeable and thus become fodder for domestic-policy debates.

If this link between domestic policy and international human rights is indeed a novel feature of debates like that over encryption, what accounts for it? Partly it is a function of the globalized media environment. Partly it stems from the fact that the European Union has directly conditioned transatlantic data flows on its approval of US surveillance practices and data-privacy guarantees. Most of all, however, it is a function of the fact that the same products and services, controlled by the same relatively small set of multinational (but principally American) technology giants, are used around the world, with business models that transcend borders.[14]

These transnational business models mean that the US government's regulatory, surveillance, or law-enforcement practices on US soil alter the terms on which a foreigner overseas interacts with US-made (or, more accurately, US-regulated) technology. For example, the scope of the government's authority under Section 702 of the FISA Amendments Act of 2008 affects how much data about a foreign Facebook user the US government can obtain from Facebook for foreign-intelligence purposes.[15] Yet even though the relevant actions all take place on US soil, Facebook's custody of that data, and the US government's access to it, directly implicate the user's own government's interests in several legitimate respects. Specifically, they implicate that government's own potential national-security or law-enforcement interests in the content of the data; its interest (whether aligned, as in the case of counterterrorism cooperation, or antagonistic, to the extent that US access raises counterintelligence concerns) in the fact that the US government is able to access and exploit it; and its interest in regulating, from a privacy perspective, the terms on which private companies handle its citizens' data, perhaps best illustrated by the saga of the US-EU data-transfer accord recently reincarnated as Privacy Shield.

Of course, all of this also interacts with foreign governments' own illegitimate interests in preferring their own local technology companies to American competitors. And it is often difficult to tease out this improper protectionist motive from more legitimate concerns over data privacy or domestic security. For example, China "has a long history of using encryption policy to foster national and domestic security as well as to promote economic growth and indigenous innovation," with ostensibly security-related regulations "also be[ing] deployed as part of a larger effort to use standards policy to bolster the competitiveness of Chinese technology firms."[16] Deutsche Telekom, 31.7 percent of which is owned by the German government,[17] seized on the Edward Snowden revelations in an attempt to divert German demand from US providers to its own telecommunications

services.[18] One prominent example was a service advertised as E-mail Made in Germany, launched just months after the Snowden revelations.[19]

It is not surprising when these competing national interests manifest themselves as competing regulatory obligations—or, at a minimum, regulatory pressures[20]—for the companies whose products or services are involved. In short, decisions made by the United States, even if intended to have legal effect only within the United States, increasingly affect the interests of both users abroad and their governments.

Domestic Needs and Global Aspirations

The encryption debate illustrates well the tension between the US government's internal law-enforcement and counterterrorism needs and its global, values-driven aspirations for the future of information technology. It also shows the difficulty of keeping these spheres separate.

Law-Enforcement and Counterterrorism Needs

On the domestic side, user-controlled encryption offers little upside for the US government. Government agencies, like most companies, don't want their employees to have sole access to the data stored on their government-issued devices or to the contents of their official communications. While encryption, broadly speaking, enhances information security, *end-to-end* encryption that precludes third-party intermediaries like Google or Microsoft from scanning messages for spam, viruses, or child pornography may be net-neutral or even net-negative for the government's cybersecurity and law-enforcement goals. And officials' private use of encrypted messaging services could present counterintelligence risks.

Meanwhile, the downsides of user-controlled encryption for law enforcement and counterterrorism are by now well-documented. The most prominent manifestation is Apple's introduction of user-controlled full-disk encryption on iPhones running iOS 8 or later. The FBI famously sought to compel Apple to help it break into an encrypted iPhone owned by San Bernardino County but protected by a password chosen by the county's employee, San Bernardino shooter Syed Farook. Investigators ultimately gained access to the phone after the FBI paid roughly $1 million for an exploit bought from an unnamed private actor.

The widely publicized San Bernardino case is only the most prominent example of an expanding challenge. Law-enforcement agencies around the United States, and increasingly the world, are accumulating piles of encrypted smartphones that they suspect contain evidence of serious crime, but which neither they nor the device's manufacturer can open, even with a judicial order. The challenge is especially severe for America's thousands of local law-enforcement agencies. While the FBI may have the resources to buy gray-market exploits in high-profile counterterrorism cases, local police departments investigating "routine" murder and rape cases don't.

Supporters of user-controlled encryption often point to metadata and cloud backups as alternative sources of evidence available to law enforcement. Law-enforcement officials counter that these are incomplete solutions. Cloud backup may have been disabled or may not yet have captured the most recently created (and thus most probative) data. Deleted data—again, often among the most probative evidence—can sometimes be recovered from a device, but cannot be recovered from the cloud.[21] Metadata are simply not as probative as the content of messages. And government access to metadata raises its own privacy concerns, which are only beginning to be confronted.

Finally, the rise of end-to-end encryption of messages in transit raises the stakes for access to data at rest on devices. When a suspect uses a cloud-based messaging service that is not end-to-end encrypted, law enforcement can simply obtain a judicial order compelling the provider to hand over the messages. But if the provider cannot access the content of the messages, the only way for law enforcement to read them is on the device, by essentially placing itself in the position of the end user. If the user is still actively using the phone, the government can do this by getting a warrant to place spyware on the phone, by using subterfuge to learn the passcode or seize the device while unlocked, or potentially by compelling the user to unlock the phone with a fingerprint if the phone is equipped with Apple's Touch ID.[22] Once the user is dead or otherwise unavailable, however, so is the password, making the phone effectively a brick. This makes it impossible to discover the content of messages transmitted using end-to-end encrypted services.[23]

Internet-Freedom Aspirations

From the perspective of the US government's international role as a promoter of democratic movements and freedom of conscience, however, encryption and anonymization tools take on an entirely different coloration. Unfortunately, journalists, activists, and dissidents living under regimes with weak commitments to the rule of law have a very real need for technologies that hide their communications and online activities from prying eyes.

Technologically sophisticated authoritarian great powers like Russia and China, of course, have built their own highly advanced surveillance systems to monitor dissidents, opposition groups, and members of disfavored minorities. Increasingly, however, less sophisticated authoritarian governments are also in the surveillance game, deploying high-tech monitoring systems and hacking tools that they buy from private companies. For example, the Associated Press recently reported that a number of governments used "lawful intercept" tools made by Verint Systems, headquartered in Melville, New York, to spy on dissidents, opposition politicians, and journalists.[24] According to leaked documents, the system Verint installed for Peru allowed Peruvian officials to easily " 'intercept and monitor' satellite networks that carry voice and data traffic."[25] Another company sold to Uzbekistan tools that "let Uzbek secret police quickly locate and arrest people who discuss sensitive information on the phone or via email."[26]

Perhaps the most infamous example is Hacking Team, an Italian spyware firm that sells sophisticated hacking tools to governments around the world. In a schadenfreude-inducing twist, Hacking Team itself was hacked in 2015 by an anonymous online vigilante. The hacker then dumped 400 gigabytes of internal company files onto the Internet. The documents revealed that Hacking Team sold its software to various regimes with questionable or poor human-rights records, including Azerbaijan, Bahrain, Egypt, Ethiopia, Kazakhstan, Morocco, Nigeria, Oman, Saudi Arabia, and Sudan, which is subject to a UN arms embargo.[27] Internet-freedom activists investigating Hacking Team have identified specific incidents where Hacking Team's tools were used against identifiable peaceful dissidents. In one case, the United Arab Emirates apparently used a Hacking Team tool to "take over [the] computer and record every keystroke" of Ahmed Mansour, a pro-democracy activist in Dubai.[28] Mansour later "suffered two beatings by thugs . . . during his campaign for citizens' civil rights" in the UAE.[29] Foreign governments have even used Hacking Team's software to hack and surveil regime opponents living in the United States.[30]

There are inchoate efforts to prevent the transfer of these potentially invidious technologies to regimes with poor human-rights records. The Wassenaar Arrangement, an export-control regime with forty-one signatories, mostly OECD (Organisation for Economic Co-operation and Development) countries, restricts the export of commercial hacking tools. In the wake of the Hacking Team revelations, Italy, a Wassenaar member, revoked the company's "global authorization" to export its products.[31] Yet the movement of software is difficult to control and surveillance "technologies continue to be exported to countries that are known human rights violators" despite the Wassenaar rules.[32]

Much of the software sold by these companies is not particularly advanced compared to the tools deployed by the most sophisticated governments. These companies' principal "value add," so to speak, is not the technology itself but rather making it accessible to technologically unsophisticated governments. As the hacker who exposed Hacking Team colorfully explained: "What they provide is packaging it all in some point-and-click way and providing all the technical support. So shitty dictators that can barely turn on a computer can hack and spy on their opposition."[33] This means that the human-rights challenge is not solely, nor even principally, driven by governments that are technologically sophisticated. Even tin-pot dictators are now able to hack and surveil, with alarming ease.

With surveillance and hacking tools now widely used as instruments of repression, it is natural that Internet freedom has become an integral and visible element of the United States' broader international human-rights agenda. The US government annually funds the development of secure communications technologies for use by dissidents overseas, primarily through the State Department's Bureau of Democracy, Human Rights, and Labor (DRL). For example, DRL's most recent Internet Freedom Annual Program Statement invited organizations to apply for funding for the "[d]evelopment and support of desktop and mobile technologies that . . . enable secure communications."[34]

The US government's most famous contribution to robust information privacy—or, depending on one's perspective, lamentable law-enforcement blindness—is Tor, free and widely used software enabling users to browse the Internet anonymously and create "hidden services" whose URLs are invisible to the public.[35] The Naval Research Laboratory developed, and later released to the public, the code that underpins Tor, and the US government has given the Tor Project millions of dollars of funding over the years. Somewhat less well-known, but more relevant here, is that the government contributed millions of dollars to develop the encryption protocol used by the secure messaging service Signal and now also by WhatsApp.[36]

These technological contributions have been matched by stepped-up diplomatic efforts. The United States is a founding member of the Freedom Online Coalition, a group of governments committed to "support[ing]—both politically and through project aid—the ability of individuals, particularly those operating in repressive environments, to exercise their human rights through the Internet and connection technologies."[37] Secretary of State John Kerry has described Internet freedom as "a point of separation between governments that want the Internet to serve their citizens and those who seek to use or restrict access to the Internet in order to control their citizens."[38] Assistant Secretary of State Tom Malinowski, head of DRL, reminded an audience of what he called "Internet freedom fighters" attending a State-sponsored Internet freedom conference last fall that over the course of the Obama administration, the State Department has "invested more than $125 million to help give ordinary people and defenders of human rights practical tools to stay ahead of Internet censors" and that these tools "enable millions of users living in Internet-censored countries to safely access the Internet each year."[39]

This commitment is only becoming more salient; even as the FBI pushes back against user-controlled encryption, the State Department is expanding its efforts to make the Internet more difficult to monitor and control. US Ambassador to the United Nations Samantha Power announced at the aforementioned State-sponsored Internet freedom conference a new Leading Internet Freedom Technology (LIFT) initiative which aims to develop "innovative next-generation technologies," not merely "to circumvent Internet censorship" but also "to make the Internet inherently . . . more resistant to control."[40] The new LIFT initiative is "part of an overall increase in the State Department's annual funding for Internet freedom to $33 million."[41] Democratic presidential nominee Hillary Clinton has promised to "continue this work as President—fighting for Internet Freedom, insisting nations respect human rights online, and opposing efforts to block internet access or shutdown social media."[42]

Finally, it bears noting that many of the outside advocates pressing the case for encryption as a human-rights tool are not simply passive critics but have actively invested their own financial and human resources in the cause. To take just a few prominent examples: Google's holding company, Alphabet, has created an internal "incubator," now known as

Jigsaw, whose raison d'être is to develop software to empower activists and investigative journalists and protect them from government surveillance.[43] The nonprofit Tor Project has received funding not just from the US government (and other like-minded governments, including Germany and Sweden), but from an array of privacy groups, like the Electronic Frontier Foundation; private foundations, including the National Christian Foundation; companies like Google and Reddit; and tens of thousands of individual donors.[44] The Electronic Frontier Foundation has developed and distributes its own browser add-on, HTTPS Everywhere, to facilitate secure Internet browsing.[45] These private actors have invested directly in the international Internet-freedom agenda—pitting their own resources against those of the Hacking Teams and Verints of the world—and thus form a powerful domestic constituency for factoring international human-rights consequences into the domestic encryption debate.

The US Government's Domestic-International Divide on Encryption and Anonymization: Hypocrisy or Principled Distinction?

Of course, the irony, as some see it, is that the national-security and law-enforcement arms of the government are simultaneously struggling against the very systems that DRL has funded for years with millions of dollars of taxpayer funds. (An alternative account is that this internal tension, with the government simultaneously carrying out two equally valid missions that are in tension with one another, is a feature of the system, not a bug.) The FBI's struggle against user-controlled encryption, described briefly above, is well-known. Less prominent is law enforcement's struggle against Tor, which has provided a sanctuary not just for human-rights activists, but also for less wholesome online activities. Since 2014, the FBI has notched a series of high-profile victories against hidden websites, accessible only using Tor, that peddled contraband on what is known as the Dark Web.

First, the FBI took down a series of "dark markets" facilitating trade in contraband like drugs, stolen credit-card data, fake identity documents, counterfeit currency, and firearms.[46] Most prominent among these were Silk Road and its successor, Silk Road 2.0, sites on the Dark Web where users could anonymously purchase drugs in Bitcoin.[47] Significantly, the FBI reportedly accomplished the Silk Road 2.0 takedown by systematically undermining Tor's anonymizing infrastructure.[48]

More recently, the FBI launched a massive operation to identify and prosecute users of an odious Dark Web child pornography site, Playpen. Acting on a tip from a foreign law-enforcement agency, the FBI located and seized the site's server and then operated the site for two weeks from a government warehouse in Newington, Virginia.[49] During that period, the FBI apparently served custom-built spyware to users who accessed sections of the site that hosted illegal content. That FBI-inserted software reported back to the government the user's IP address and other information about the user's computer and logged the data transmitted between the user's computer and the Playpen server. The government has since

commenced more than one hundred prosecutions based on this operation, although in several cases its evidence has been suppressed or excluded for reasons not relevant here.[50]

The US government's pivotal role in developing and disseminating powerful encryption protocols and Tor have led privacy and technology advocates to criticize what they see as a schizophrenic approach to these technologies. Yet the government's seemingly inconsistent actions are not necessarily irrational. The US government, one might argue, is bound both by hard law, constitutional and statutory, and by soft but nonetheless behavior-shaping rule-of-law norms that constrain how and why government officials access private data. By contrast, authoritarian regimes, the targets of the United States' international Internet-freedom agenda, are not similarly constrained. So it is not necessarily hypocritical or internally contradictory for the United States to seek to circumvent encryption and anonymization in pursuit of its own law-enforcement needs and simultaneously to encourage their use against authoritarian governments.

Of course, many argue that the government should not, even as a matter of pure domestic policy, seek to compel companies to retain the capability to decrypt messages carried by their services or data stored on devices they manufactured, whether by legislation like the proposed Burr-Feinstein bill[51] or by obtaining case-specific court orders.[52] They argue, *inter alia,* that introducing additional insecurities into technology products harms, in various ways, the security of the United States, its allies, its companies, and its citizens—for example, by weakening defenses against cyber-crime and cyber-espionage.[53] There are also colorable arguments that the First Amendment protects the rights to disseminate cryptographic source code[54] and to transmit one's own correspondence in code.[55] But even if it would be constitutional, a government mandate that citizens transmit their correspondence in a manner designed to facilitate surveillance would, at least arguably, be hard to square with American history and values. Thomas Jefferson, famously, was an enthusiastic amateur cryptologist, even inventing his own wheel cipher.[56] And it is not difficult to imagine how the Framers would have responded to a British edict prohibiting colonists from encoding their letters.

There may also be those who are ideologically committed to the view that no degree of domestic exigency would outweigh the United States' international human-rights mission. Or, put more aggressively, that the United States' obligation to stand with dissidents and human-rights advocates living under authoritarian regimes should always trump self-interested instrumental considerations, no matter how weighty. If one views these arguments, whether in isolation or combination, as dispositive, one need not wrestle with the tension between legitimate domestic goals and international aspirations. For that reason, we set these arguments aside here, without further comment on their merits.

Assuming, then, that domestic goals and international aspirations are in tension, how should decisionmakers approach the task of reconciling them?

Toward a Pragmatic Approach

One disappointing aspect of the domestic encryption debate is that it has been waged on terms that are almost exclusively ideological rather than pragmatic and factual. Both sides of the debate bear some responsibility for this.

Government officials frequently imply that the Fourth Amendment resolves the dispute in their favor as a matter of principle. Specifically, they contend that maintaining the Fourth Amendment's "balance" requires that all evidence be amenable to search pursuant to a valid warrant.[57] Meanwhile, the factual record that might bolster the government's case for a decryption mandate is not as developed as it might be.[58] Before Congress enacted the Communications Assistance to Law Enforcement Act (CALEA) in 1994, analysts from the (since-renamed) General Accounting Office "interviewed technical representatives from local telephone companies, switch manufacturers, and cellular providers, as well as the FBI" and presented their results to Congress.[59] The House Report on CALEA then broke down by specific technical cause 183 incidents in which law enforcement encountered problems in implementing "authorized electronic surveillance."[60] Law enforcement could strengthen its case for a decryption mandate today by providing analogous detail about the specific technical obstacles (e.g., device and operating-system versions) and surrounding circumstances (e.g., whether a cloud backup was available and why it was insufficient) encountered in the many cases where investigations have reportedly been impeded by encryption.

For their part, encryption advocates argue that a requirement that companies retain the ability to decrypt messages transmitted over their services or data stored on devices they manufacture would render those technologies inherently, intolerably unsafe. Yet surely it is possible to investigate with greater precision *how much less safe* such a mandate would make this data.[61] It must be possible to review, for example, whether earlier versions of device operating systems did or did not result in unauthorized access by criminal actors and adversary states. And it should be possible for technologists to undertake a forward-looking, practical assessment of how great the reduction in security would be if such a mandate were enacted. How frequently would criminal actors in physical possession of a user's phone also have the technical capability to penetrate encryption keyed to the user's passcode, which the manufacturer alone, using its private key, retained the ability to circumvent? One way for advocates (and neutrals) to advance the process of concretizing the additional risk created by such a mandate is to propose specific forms that an exceptional-access mechanism might take, as security researcher Matt Tait has done.[62]

It may very well be that the answers to these questions would demonstrate overwhelmingly that a decryption mandate would be a security disaster, as opponents contend. But it would be helpful to know.

Analyzing the International Effects of a Domestic Decryption Mandate

What value those willing to weigh the costs and benefits of a decryption mandate—that is, those not ideologically pre-committed to oppose or support such a law—should assign to its potential international effects similarly depends, at least in part, on potentially knowable facts about the world. The argument that the United States should, in the name of Internet freedom and international human rights, forswear a tool that is (for purposes of argument) valuable to domestic law enforcement and counterterrorism rests on the premise that what the United States does domestically will in fact have either significant positive or negative effects overseas.

This may be true, but it is not self-evident. It is possible that if the United States forswears "backdoors" or mandatory decryption, that example will meaningfully influence other countries as they formulate their reactions to user-controlled encryption.[63] On the other hand, it may be that other countries' own domestic and international security interests in accessing encrypted data are so strong that they will plow ahead regardless of what the United States does. Brazil, for example, has repeatedly shut down WhatsApp over the issue of law-enforcement access to encrypted messages.[64] China permits only encryption products approved by the Office of State Commercial Cryptography Administration, whose approval standards are readily imagined.[65] More broadly, Adam Segal notes that China's technology policy reflects its powerful interests in regime stability and promotion of domestic alternatives to foreign technology—both of which cut strongly against allowing foreign companies to sell in China products that are not "secure and controllable" by the Chinese state.[66] The increasing availability of high-quality Chinese substitutes for foreign IT products is another factor rapidly eroding what Segal calls "[t]he ability of foreign companies and governments to get Beijing not to do something it wants."[67]

Indeed, even some liberal democracies have shown an independent inclination toward mandatory decryption. Britain's government proposed mandatory decryption in its recent draft Investigatory Powers Bill; the final version retreated somewhat but still provides that companies can be "asked to remove encryption that they themselves have put in place" as long as "doing so is technically feasible and not unduly expensive."[68] France's National Assembly is currently considering substantially increasing penalties for companies who refuse to assist law enforcement in decrypting messages related to crimes under investigation.[69]

It may be that the most probable outcome is somewhere in the middle: major unaligned or adversary states, like Brazil and China, are likely to set their own course without regard to what the United States does. Governments that have foresworn or consciously declined to seek mandatory decryption—Germany, for example, has opted to create a new agency to assist law enforcement in unilateral codebreaking rather than attempt to mandate backdoors[70]—will draw succor from the United States' decision. Governments inclined to

oppose mandatory decryption but wavering in the face of domestic political pressure might gain some political capital from the United States' decision to forswear it. An additional risk to consider is that if liberal democracies like Britain and France adopt anti-encryption legislation, they will provide adequate rhetorical cover for authoritarian regimes despite the United States' self-denial, neutralizing some of the hoped-for benefits of such abstinence.[71]

One confounding factor in assessing the potential international effects is that the United States' domestic approach to strong encryption is likely to be most influential in *non-authoritarian* countries—that is, in like-minded liberal democracies with strong rule-of-law cultures. Whether one considers influencing domestic encryption policy in, say, Germany and France a desirable effect of US policymaking depends on whether one views the privacy conferred by strong encryption as (1) inherently good or (2) variably good or bad depending on whether or not the access it obstructs is legitimately motivated and authorized by law. That is to say, it will likely track one's views on the domestic question of whether or not it is desirable for law enforcement to be able to access encrypted data where it is covered by a search warrant. It seems fair to assume, however, that most Americans who are not technologists or privacy advocates would not consider obstructing French or German law enforcement's access to encrypted data a valid US policy goal or a net gain for international human rights.

A second key area of uncertainty is the effect that a US decryption mandate would have on the range of products available in the marketplace. US companies are responsible for many, albeit not all, of the most secure communications technologies that are widely available to consumers. Apple's iOS devices are generally considered to be the safest consumer devices available. According to security researcher Nicholas Weaver, "[p]roperly configured, an iOS device is perhaps the most secure, general purpose communication device available. . . . [A]n iPhone configured with a proper password has enough protection that, turned off, I'd be willing to hand mine over to the DGSE, NSA, or Chinese."[72] The Australian government has even certified iOS devices to handle classified government communications.[73]

If the United States were to mandate that iPhones sold domestically contain some kind of access mechanism, it seems safe to assume that authoritarian regimes would soon permit Apple to sell only that "backdoored" US-edition iPhone in their markets. As Senator Ron Wyden (D-OR) has argued: "[I]f the FBI can force Apple to build a key, you can be sure authoritarian regimes like China and Russia will turn around and force Apple to hand it over to them."[74] If the chosen exceptional-access mechanism resembled Matt Tait's "cryptographic envelopes" proposal, with the US government holding one of multiple keys required to open passcode-protected phones sold in the United States, then China, Russia, and other countries with substantial market power would likely demand that a similar access mechanism be built into phones sold in their countries.[75]

Alternatively, were decryption legislation to adopt the type of "performance standard" sought by FBI Director James Comey (i.e., a requirement that companies provide clear text

upon receipt of lawful process without specifying the mechanism), the technical state of play would effectively revert to where it was before iOS 8: unless a government could spoof or steal Apple's private key—the likelihood of which is itself an unknown variable here[76]—governments would have to send seized password-locked iPhones to Apple for it to extract the stored data. Apple's guidelines for US law enforcement describe how this process works for devices running operating systems up to iOS 7:

> For iOS devices running iOS versions earlier than iOS 8.0, upon receipt of a valid search warrant issued upon a showing of probable cause, Apple can extract certain categories of active data from passcode locked iOS devices. Specifically, the user generated active files on an iOS device that are contained in Apple's native apps and for which the data is not encrypted using the passcode ("user generated active files"), can be extracted and provided to law enforcement on external media. Apple can perform this data extraction process on iOS devices running iOS 4 through iOS 7. Please note the only categories of user generated active files that can be provided to law enforcement, pursuant to a valid search warrant, are: SMS, iMessage, MMS, photos, videos, contacts, audio recording, and call history. Apple cannot provide: email, calendar entries, or any third-party app data.[77]

If Apple retained the capability to decrypt passcode-locked iPhones, it would be forced to choose whether to comply with similar requests from foreign governments, taking into account the legality and legitimacy of the request and the cost of defying the requesting government—much as companies do today when confronted with foreign-government requests for communications metadata.[78] Users in China will likely be out of luck; users in Zimbabwe will probably be safe.

Refereeing such foreign-government requests is obviously an awkward and undesirable position in which to place Apple and other similarly situated companies—something Congress should certainly take into account as it considers legislation. Setting that aside, however, from a pure human-rights perspective it is fair to ask how much worse that scenario would be than the status quo. Much criticism of the FBI's quest for a decryption mandate rests on the premise that such a measure would, again quoting Senator Wyden, "give repressive regimes in Russia and China a blueprint for forcing American companies to create a backdoor."[79] Yet powerful authoritarian states are already able to dictate the terms of access to their markets and, it appears, compel access.

China, as noted above, permits only government-approved encryption technologies to be sold in the country and subjects Western companies to intrusive "security reviews" before permitting consumer technologies to be sold in China.[80] Some observers suspect that iPhones sold in China may already be less secure than those sold in the United States, whether through the China-specific WAPI wireless protocol or some other mechanism.[81] Russia has already mandated that companies store Russian users' data domestically[82] and has begun auditing American companies' compliance with these data-localization

requirements.[83] It also recently finalized a new law that will require firms to decrypt communications or face heavy penalties.[84] These countries may condition access to their markets on access to users' data regardless of what the United States does.

Weak authoritarian states, however, will not have the same market power. Even if China and Russia succeed in making all domestic communications transparent to their security services, a pro-encryption policy might nonetheless be deemed a success if it prevents the Ethiopias and Uzbekistans of the world from surveilling and repressing their dissidents and journalists.[85]

A third unknown variable is how resilient the United States' global Internet-freedom agenda might be despite a domestic choice to impose a decryption mandate. Critics would call this hypocrisy; defenders would see it as a justifiable distinction given the United States' domestic constitutional protections and relatively robust oversight regime. It may be that such "hypocrisy," as it were, is a viable course of action—that it is feasible, as a practical matter, to maintain diplomatic and moral pressure on authoritarian states while simultaneously imposing a decryption mandate in the United States. It is safe to assume that authoritarian regimes would use the United States' decision as rhetorical cover for their own domestic digital repression. But many, like Russia and China, would have taken the same actions even without the United States as a convenient excuse. Others would lack the technical sophistication to circumvent widely available encryption technologies or the market power to force companies to do it for them. And some weak authoritarian states might succumb to international pressure not to take such steps, particularly if this pressure were backed by diplomatic or economic consequences. Another factor is whether export-control regimes like the Wassenaar Arrangement can successfully prevent companies from selling hacking tools to technologically unsophisticated regimes that would struggle to circumvent user-controlled encryption on their own.

One unfortunate aspect of the current debate has been the failure of the various arms of the US government with equities at stake in the encryption debate to coordinate their positions and reconcile their arguably competing interests. To the extent that US officials view a domestic decryption mandate as consistent with the State Department's international Internet-freedom agenda, they should explain why, in their view, the former would not adversely affect the latter, and what steps the US government would take to protect the Internet-freedom agenda from any potential spillover effects. This would help neutral observers form a more accurate, factually informed judgment about the likely human-rights consequences of an aggressively regulatory domestic approach to user-controlled encryption.

How Important Are International Effects in the Larger Encryption Debate?

Ultimately, the conclusions an open-minded observer draws about the international implications of the encryption debate should follow from the answers to questions like

those suggested above. How powerful an influence does the United States' example exert? What effect would a domestic decryption mandate have on the security of products sold in other countries? And how feasible would it be to maintain diplomatic and moral pressure on authoritarian states while simultaneously imposing a decryption mandate in the United States? If the causality is weak—if (a) the United States' domestic actions exert little influence internationally, (b) other countries' determination to break encryption and unmask Internet users is sufficiently strong to overcome any US influence, or (c) a strong global Internet-freedom agenda can overcome most of the drag exerted by a domestic decryption mandate—then international effects should carry relatively little weight in the overall equation. Conversely, if US actions exert a strong causal effect on developments internationally, those international consequences should carry relatively more weight.

Depending on the answers to these questions, one can imagine at least three possible attitudes toward international human-rights consequences as a factor in the broader encryption debate. First, one who concludes that the United States' example exerts a powerful influence abroad, or who anticipates that a decryption mandate for products sold in the United States will inevitably result in less-secure products leaking into the global market, would be more inclined to favor affirmatively disavowing decryption mandates and taking an unequivocal stance in favor of user-controlled encryption at home and abroad. (The Obama administration consciously opted not to make such a disavowal when it teed up the issue for presidential decision last year.[86]) Call this the "city on a hill" approach.

Second, if one concludes that the United States' example in this area exerts relatively little influence on other countries' behavior, or that other countries' interests in access to data are so strong that they will seek to break encryption, unmask Internet users, and so forth, in spite of whatever influence the United States can exert, one would assign little weight to international human-rights considerations in deciding whether a domestic decryption mandate is desirable. There's also a sharper-edged version of this argument: If companies will decrypt data for China and other regimes that are not bound by meaningful rule-of-law protections, why should they refuse to do so here in response to a full-dress search warrant issued by an independent federal judge? Call this the "don't be a sucker" approach.

Third, even if one believes that the United States' example exerts a powerful influence abroad, one might conclude that it is possible to influence authoritarian states' practices despite enacting a domestic decryption mandate, hacking Tor in pursuit of legitimate law-enforcement goals, or taking other arguably contradictory measures at home. Call this the "do what I say, not what I do" approach. Notwithstanding Americans' innate distaste for hypocrisy (or perceived hypocrisy), this bifurcated resolution would be rational if the underlying factual assumptions hold.

None of this is to say, of course, that it would be possible or even desirable to have a purely factual, values-free debate. Even with perfect information about the costs and benefits of

a decryption mandate, different observers would judge the desirability of the attendant trade-offs differently depending on the relative weights they assign to the competing values at stake. Some may believe that human rights are inherently more important than domestic law enforcement; others may deem stopping child sexual exploitation the highest priority. Public-policy debates cannot be reduced to a set of bloodless equations. Ultimately, the participants must consult their own normative priors to decide what interests should be pursued, and at what cost.

The goal here is thus not to purge values-based arguments from the encryption debate. Rather, it is to permit decision-makers to bring their values to bear on a more fully developed factual record and to encourage the parties to sharpen their claims so that they are more factually testable. The encryption debate would be more useful to the ultimate decision-makers were the parties to focus on generating and debating relevant facts rather than exchanging pre-baked, ideologically rooted conclusions.

Of course, many of the questions raised above call for predictive judgments, which cannot be made with absolute certainty, rather than hard, empirically validated facts. That does not mean, however, that the encryption debate resists pragmatic, factually grounded arguments. To the contrary: these are the same type of predictive judgments about other nations' anticipated behavior that analysts routinely form and rely on in making foreign policy. On encryption policy, as in other areas where the goal is to forecast other states' behavior, reasonable default assumptions are that national interest, capability, relative power, and other mostly objective and discernable factors will shape what other nations seek to do, and what they are able to do.[87] If informed by adequate information about other countries' interests, capabilities, and vulnerabilities, such forecasts are as sound a basis for policymaking in the encryption debate as they are in political, military, and economic affairs more broadly.

There is one final reason to be confident that a factually informed debate on the international implications of US encryption policy is possible. Given that the debate in the United States will almost certainly remain stalemated absent another major terrorist attack or eruption of Snowden-level revelations, the next few years will serve as a natural experiment for how other countries will approach this challenge independent of significant US action.[88] This period of waiting and observation will provide additional data on the extent to which domestic US policy is or is not a significant determinant of other countries' own domestic approaches to encryption. If major European countries impose decryption mandates or stringent technical-assistance requirements, will those mandates have spillover effects in authoritarian states? Will China, Russia, and other authoritarian powers continue to pursue aggressively regulatory approaches to encryption and user data, despite the potential economic and cybersecurity costs? Will weaker authoritarian states follow China and Russia, or are they too constrained by their technological ineptitude and economic insignificance? The experience of the next few years will add substantially to the available

set of relevant examples—perhaps an additional argument for what Benjamin Wittes terms "leading from behind on encryption."[89]

Implications for Policy–and Advocacy

None of this is to say that it is irrational or inappropriate to believe that some overweening value—whether the United States' obligations to human-rights defenders abroad or the sanctity of the search warrant—resolves the debate one way or another without regard to the strength of countervailing considerations, including a decision's potential international implications. But the parties to the encryption debate should bear in mind that while some observers will be bound to one answer or another by their ideological or institutional commitments, most will not. That includes most members of the Congress that will ultimately determine this issue one way or another, whether by action or inaction. These pragmatic persuadables are willing to accept trade-offs and imperfect outcomes—indeed, unlike many of the participants, they accept that any outcome here will be imperfect in some respect. For that reason, arguments phrased in terms of rigid principles are likely to be less persuasive than arguments focused on the specific costs that such a law would impose or the specific benefits it would confer. As Susan Hennessey has argued in analyzing the Burr-Feinstein draft:

> Preserving the technical mechanisms for access or decryption might compromise ideal security—maybe even basic security—but it's clearly possible. . . .
>
> This is an important point for those who want to dismiss the legislation as ignorant of mathematical principles. The drafters do not reject the premise that it is impossible to both have third-party access or decryption capability and also have an ideally secure system. Rather, recognizing this kind of access would result in some degree of real or theoretical lessened security, they have determined that there are ways to manage these risks. *Advocates who wish to change the minds of those who support this bill must be convincing on this point—that there is, on balance, no feasible way to manage the risk*.[90]

This holds important implications for both the parties to the debate and for those neutrals charged with resolving it. First, because most observers will follow a pragmatic, instrumental calculus in deciding whether a decryption mandate is good policy, the parties would be well advised to focus on building out a factual record to support their claims. Rather than simply stating that a decryption mandate will undermine security, technology companies and civil libertarians opposed to such a mandate should explain, in specific and concrete terms, *how* and *to what extent* it will do so, and should document comparable past intrusions. To take one example, opponents of mandated "backdoors" have pointed to the "Athens affair," in which unknown hackers exploited a lawful-wiretap mechanism in the system of Vodaphone Greece to wiretap one hundred senior members of the Greek government, including the prime minister and the ministers of defense and justice.[91] But

such anecdotal evidence, while relevant and to some extent probative, is only one element of a compelling fact-based argument.

With respect to the international aspects of the encryption debate, evidence showing that what the United States does domestically matters overseas, or that it does not, will be a powerful tool in this debate. Opponents will also want to show that "backdoored" technology developed for use by law-enforcement agencies bound by the rule of law tends to "leak out" to autocracies. The commercial surveillance industry described above may be one example of this. It will not be enough to merely argue that a domestic decryption mandate will be said to contradict the United States' Internet-freedom agenda. Rather, opponents will need to show that the distinction will be perceived as indefensible, and that this perception will in fact have real-world policy consequences—or, alternatively, that the technological reverberations of the mandate will harm international human rights even if the mandate is widely perceived as legitimate. Conversely, advocates of a domestic decryption mandate will seek to muster evidence that other countries will proceed with analogous laws regardless of what the United States does—or, more subtly, that regardless of what the United States does domestically, powerful autocracies will proceed with such laws while weaker ones can be pressured into forswearing them or will lack the technological sophistication to implement them.[92]

Finally, open-minded members of Congress should consider how they can structure the decision-making process to generate the factual record needed to inform a pragmatic legislative approach to this issue. One widely discussed option is a bipartisan outside commission, a model which in the past has generated useful policy ideas and, at times, political will to implement them. House Homeland Security Committee Chairman Michael McCaul (R-TX) and Senator Mark Warner (D-VA) have introduced legislation to create a Commission on Digital Security, which would explore the relevant facts and make policy recommendations.[93] Hillary Clinton recently echoed this, calling for a "national commission on digital security, so that the technology and public safety communities can work together on solutions that address law-enforcement needs while preserving individual privacy and security."[94] The House Energy and Commerce and Judiciary committees have pushed back, arguing that Congress, not an outside panel, is the appropriate forum to resolve this debate.[95]

Commissions and other outside inquiries, while good for some roles, are ill-suited for others. Where a policy question calls for value judgments rather than neutral fact-finding, those judgments are more appropriately made by the people's elected representatives in Congress than by unelected commissioners. Congress's competence and efficiency may be held in low esteem, yet only Congress has the representative legitimacy needed to settle a dispute involving such core American values and interests. On the other hand, commissions can usefully support the legislative process, even on such hot-button issues, by developing an authoritative factual record, bearing a bipartisan imprimatur, from which the debate

can proceed. Commissions can also usefully advance the public debate by obtaining declassification of previously secret information. For example, the *9/11 Commission Report* and the Privacy and Civil Liberties Oversight Board's report on the Section 702 program both contained many previously classified details about national-security processes. If an encryption commission were tightly focused on these more modest aims, it might succeed and usefully advance the debate. Alternatively, the National Academy of Sciences has reportedly assembled a technical working group to examine the encryption issue. If so, that group's report would help support an informed, fact-based debate.

An appropriately scoped commission would have one additional virtue in this context—one that is not widely appreciated, but that should appeal to civil libertarians and others who would not welcome the type of government-empowering legislation that often emerges in the wake of major terrorist attacks. If there is another major terrorist attack in the United States, a pending commission would serve as a buffer against hasty post-attack legislation—both because Congress will be reluctant to legislate before the commission reports and because the commission will provide an alternative focal point for the enormous post-attack urgency felt by the public and the Congress. Most important here is that if such a body is ultimately formed, its mandate should include the international aspects as well. In particular, it should be tasked with answering the critical factual questions discussed above.

• • •

A decryption mandate almost certainly would not pass, no matter how compelling a case its advocates could mount, given the current political balance of power. Yet tomorrow's alignment may not resemble today's. As Office of the Director of National Intelligence General Counsel Robert Litt noted last year in an email later leaked to the *Washington Post,* while "the legislative environment is very hostile today, it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement."[96] Or it could turn if November's election produces a president less sensitive to privacy, civil liberties, and the concerns of the technology industry. The encryption debate, seemingly stalemated for now, may one day reopen. Both sides would do well to begin mustering their facts now.

NOTES

1 Cf. prepared statement of Deputy Attorney General Sally Quillian Yates before the Senate Judiciary Committee, July 8, 2015 ("recent technological innovations threaten [the Fourth Amendment's] careful balance" "between privacy rights and public safety").

2 Compare Berkman Center for Internet and Society, Harvard University, "Don't Panic. Making Sense of the 'Going Dark' Debate," February, 2016, with Manhattan District Attorney's Office, report on "Smartphone Encryption and Public Safety," November 2015, http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

3 See discussion below on law-enforcement arguments.

4 "Embassy Espionage: The NSA's Secret Spy Hub in Berlin," *Der Spiegel,* October 27, 2013, http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

5 "Hunting American Spooks: Germany Prepares Further Spying Clampdown," *Der Spiegel,* July 14, 2014, http://www.spiegel.de/international/germany/expulsion-of-cia-head-a-sign-of-tougher-german-response-to-spying-a-980912.html.

6 "Spying Close to Home: German Intelligence Under Fire for NSA Cooperation," *Der Spiegel,* April 24, 2015, http://www.spiegel.de/international/germany/german-intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html.

7 See Robert G. Livingston, "Spies Get Between Germany and the United States," *AICGS Advisor,* July 15, 2014, Draft Law on Foreign-Foreign Telecommunications Surveillance by the BND § 13, https://netzpolitik.org/2016/das-neue-bnd-gesetz-alles-was-der-bnd-macht-wird-einfach-legalisiert-und-sogar-noch-ausgeweitet/.

8 See German Federal Ministry of the Interior, "Federal Minister of the Interior Travels to the United States for Political Talks," May 19, 2015 (announcing "Memorandum of Understanding that will enable Germany and the United States to improve counter-terrorism cooperation and share more information about suspects").

9 Eric Schmitt, "U.S. Officials Met With Belgians on Security Concerns Before Attacks," *New York Times,* April 4, 2016.

10 See, e.g., Laurens Cerulus, "Belgium's Clawless Terror Hawk," POLITICO EU, April 8, 2016.

11 Sebastian Rotella, "ISIS via WhatsApp: 'Blow Yourself Up, O Lion,' " *ProPublica,* July 11, 2016.

12 See Susan Hennessey, "The Elephant in the Room: Addressing Child Exploitation in the Going Dark Debate," Hoover Institution, Beyond Privacy and Security series paper, 2 (forthcoming 2016) (draft on file with author).

13 See discussion below of Tor and Playpen.

14 Cf. Milton Mueller, "What's Really at Stake in the Microsoft v. USA Decision," Internet Governance Project, July 15, 2016, http://www.internetgovernance.org/2016/07/15/whats-really-at-stake-in-the-microsoft-v-usa-decision/ (describing natural lack of "alignment" between "cyber domain" and "existing legal-political jurisdictions" and resulting governmental attempts to "superimpose[d] the authority of territorial states over the global virtual space created by the Internet").

15 See 50 U.S.C. § 1881a.

16 See Adam Segal, "China, Encryption Policy, and International Influence," Hoover Institution, Beyond Privacy and Security series paper, 1–4 (forthcoming 2016) (draft on file with author).

17 Deutsche Telekom, "Shareholder Structure," https://www.telekom.com/shareholder-structure.

18 See Friedrich Geiger, "Deutsche Telekom's Answer For Germans Spooked by NSA Spooks," *Wall Street Journal,* January 29, 2015, http://blogs.wsj.com/digits/2015/01/29/deutsche-telekoms-answer-for-germans-spooked-by-nsa-spooks/.

19 See "Boom Triggered By NSA: German Email Services Report Surge in Demand," *Der Spiegel,* August 26, 2013, http://www.spiegel.de/international/germany/growing-demand-for-german-email-providers-after-nsa-scandal-a-918651.html; see also E-mail Made In Germany, http://www.e-mail-made-in-germany.de/ ("E-Mail made in Germany offers our customers a high standard of security and data protection and stands for product quality and reliability").

20 See Paul Mozur and Jane Perlez, "China Quietly Targets U.S. Tech Companies in Security Reviews," *New York Times,* May 16, 2016 ("Chinese authorities are quietly scrutinizing technology products sold in China by Apple and other big foreign companies, focusing on whether they pose potential security threats to the country").

21 "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," written testimony of New York County District Attorney Cyrus Vance Jr. before the Senate Judiciary Committee, July 8, 2015, http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf; see also Manhattan District Attorney's Office, "Smartphone Encryption and Public Safety," November 2015.

22 But see Jose Pagliery, "FBI wasn't able to unlock iPhone, even with a 'fingerprint unlock warrant,' " CNN, May 12, 2016 (noting that this technique failed the two times it was tried and noting constitutional argument that this violates the Fifth Amendment).

23 See Cyrus Farivar, "If FBI busts into seized iPhone, it could get non-iCloud data, like Telegram chats," *Ars Technica,* February 21, 2016, http://arstechnica.com/tech-policy/2016/02/if-fbi-busts-into-seized-iphone-it-could-get-non-icloud-data-like-telegram-chats/.

24 Frank Bajak and Jack Gillum, "Snapping up cheap spy tools, nations 'monitoring everyone,' " Associated Press, August 2, 2016, http://bigstory.ap.org/article/f799cfd080b04b93a34df61fc007b096/snapping-cheap-spy-tools-nations-monitoring-everyone.

25 Ibid.

26 Ibid.

27 Andy Greenberg, "Hacking Team Breach Shows a Global Spying Firm Run Amok," *Wired,* July 6, 2015, https://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/.

28 Vernon Silver, "Spyware Leaves Trail to Beaten Activist Through Microsoft Flaw," Bloomberg, October 10, 2012, https://www.bloomberg.com/news/articles/2012-10-10/spyware-leaves-trail-to-beaten-activist-through-microsoft-flaw.

29 Ibid.

30 See Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, "Hacking Team and the Targeting of Ethiopian Journalists," University of Toronto, Munk School of Global Affairs, February 12, 2014, https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/.

31 See Lorenzo Franceschi-Bicchierai, "Hacking Team Has Lost Its License to Export Spyware," *Motherboard,* April 6, 2016, https://motherboard.vice.com/read/hacking-team-has-lost-its-license-to-export-spyware; Wassenaar Arrangement, Participating States, http://www.wassenaar.org/participating-states/.

32 Bajak and Gillum, "Nations monitoring everyone" (quoting Member of the European Parliament Marietje Schaake).

33 Lorenzo Franceschi-Bicchierai, "Hacker 'Phineas Fisher' Speaks on Camera for the First Time—Through a Puppet," *Motherboard,* July 20, 2016, https://motherboard.vice.com/read/hacker-phineas-fisher-hacking-team-puppet.

34 US Department of State, Bureau of Democracy, Human Rights and Labor, "Request for Statements of Interest: DRL Internet Freedom Annual Program Statement," June 13, 2016, http://www.state.gov/j/drl/p/258418.htm.

35 Tor is an acronym for "The Onion Router."

36 See Jeff Stone, "U.S. Government Funded The WhatsApp Encryption," *Vocativ,* April 8, 2016, http://www.vocativ.com/307106/whatsapp-encryption/.

37 Freedom Online Coalition, http://www.freedomonline.ee/about-us/Freedom-online-coalition.

38 John F. Kerry, remarks at Korea University, Seoul, South Korea, May 18, 2015, http://www.humanrights.gov/dyn/2015/05/secretary-kerry-delivers-a-speech-about-internet-freedom-and-cybersecurity-before-an-audience-at-korea-university/.

39 US Department of State, "Excerpts: Assistant Secretary Malinowski at the Internet Freedom Technology Showcase: The Future of Human Rights Online," New York, September 26, 2015, http://www.humanrights.gov/dyn/2015/10/assistant-secretary-malinowski-at-the-internet-freedom-technology-showcase-the-future-of-human-rights-online/.

40 Samantha Power, "Remarks at the Internet Freedom Technology Showcase: The Future of Human Rights Online," New York, September 26, 2015, http://usun.state.gov/remarks/6836.

41 Tom Malinowski, "The Leading Internet Freedom Technology (LIFT) Initiative: Scaling Up U.S. Leadership to Promote Human Rights Online," *Dipnote* (blog), October 12, 2015, https://blogs.state.gov/stories/2015/10/12/leading-internet-freedom-technology-lift-initiative-scaling-us-leadership-promote.

42 "Hillary Clinton's Initiative on Technology & Innovation," https://www.hillaryclinton.com/briefing/factsheets/2016/06/28/hillary-clintons-initiative-on-technology-innovation-2/.

43 See, e.g., Shane Huntley and Jonathan Pevarnek, "The Most Important Gmail Update You'll Hopefully Never See," Jigsaw, March 24, 2016, https://medium.com/jigsaw/the-most-important-gmail-update-you-ll-hopefully-never-see-673b8ffe539e#.avh643kb1.

44 See Tor Project, Sponsors, https://www.torproject.org/about/sponsors.html.en.

45 Electronic Frontier Foundation, HTTPS Everywhere, https://www.eff.org/https-everywhere.

46 See FBI, "More Than 400. Onion Addresses, Including Dozens of 'Dark Market' Sites, Targeted as Part of Global Enforcement Action on Tor Network," news release, November 7, 2014, https://www.fbi.gov/news/pressrel/press-releases/more-than-400-.onion-addresses-including-dozens-of-dark-market-sites-targeted-as-part-of-global-enforcement-action-on-tor-network.

47 See Russell Brandom, "Feds found Silk Road 2 servers after a six-month attack on Tor," *The Verge,* January 21, 2015, http://www.theverge.com/2015/1/21/7867471/fbi-found-silk-road-2-tor-anonymity-hack.

48 See Kashmir Hill, "The attack that broke the Dark Web—and how Tor plans to fix it," *Fusion,* November 30, 2015, http://fusion.net/story/238742/tor-carnegie-mellon-attack/.

49 Affidavit of Special Agent Douglas Macfarlane in No. 1:15-SW-89, at 29 (E.D. Va. Feb. 20, 2015).

50 See Hennessey, "Elephant in the Room," 14–17 (describing disputes in Playpen prosecutions over Federal Rule of Criminal Procedure 41 and defendants' requests to inspect government source code).

51 Discussion draft, "Compliance with Court Orders Act of 2016," http://www.burr.senate.gov/imo/media/doc/BAG16460.pdf.

52 See "In re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203," No. 5:16-cm-00010-SP (C.D. Cal. 2016).

53 See, e.g., Kevin Bankston, policy director, New America's Open Technology Institute, statement before the House Oversight and Government Reform Subcommittee on Information Technology, April 29, 2015, 4, 7-10 ("Whether you want to call it a front door or a back door, mandating guaranteed government access to encrypted data would open us up to a variety of new cyber-threats.").

54 Cf. Bernstein v. United States, 176 F.3d 1132 (9th Cir. 1999) (Fletcher, J.) (cryptography export controls constitute a prior restraint on speech), reh'g en banc granted and panel op. withdrawn, 192 F.3d 1308.

55 The author thanks Alex Abdo for suggesting this point.

56 Rachel Emma Silverman, "Two Centuries On, a Cryptologist Cracks a Presidential Code," *Wall Street Journal,* July 2, 2009, http://www.wsj.com/articles/SB124648494429082661.

57 See, e.g., Yates before the Senate Judiciary Committee, July 8, 2015 ("recent technological innovations threaten [the Fourth Amendment's] careful balance" "between privacy rights and public safety").

58 The author thanks Mieke Eoyang for suggesting this point.

59 H. Rept. 103-827, at 16 (1994).

60 Ibid., 16–17.

61 Susan Hennessey, "Encryption Legislation: Critics Blinded by Outrage are Blinded to the Lessons," *Lawfare* (blog), April 21, 2016, https://www.lawfareblog.com/encryption-legislation-critics-blinded-outrage-are-blinded-lessons.

62 See Matt Tait, "An Approach to James Comey's Technical Challenge," *Lawfare* (blog), April 27, 2016 (proposing "cryptographic envelopes" as a customizable and relatively secure mechanism to enable lawful access to encrypted devices).

63 See, e.g., Bankston, statement before the House Oversight and Government Reform Subcommittee on Information Technology, 13–14.

64 See Julia Leite, "WhatsApp Ordered Blocked Again in Brazil Over Data Dispute," Bloomberg, May 2, 2016, http://www.bloomberg.com/news/articles/2016-05-02/facebook-s-whatsapp-blocked-again-in-brazil-over-data-dispute.

65 Victoria White and Ingram Cheung, "China's Rules on Encryption: What Foreign Companies Need to Know," Freshfields Bruckhaus Deringer, http://www.freshfields.com/en/global/Digital/China_rules_on_encryption/ ("Foreign companies are required to report their use of any encryption technology to OSCCA, and to obtain OSCCA approval"). While this mandate applies to "products with encryption as their core function," it does not apply to products, like mobile telephones and browsers, that merely incorporate encryption.

66 See generally Segal, "China, Encryption Policy, and International Influence."

67 Ibid., 6.

68 Jeremy Kahn, "U.K. Commons Passes Controversial 'Snooper's Charter' Bill," Bloomberg, June 8, 2016, http://www.bloomberg.com/news/articles/2016-06-08/u-k-commons-passes-controversial-snooper-s-charter-bill.

69 See Daniel Severson, "Encryption Legislation Advances in France," *Lawfare* (blog), April 14, 2016, https://www.lawfareblog.com/encryption-legislation-advances-france.

70 German Federal Government, "Digital Agenda 2014-2017," 31, https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda-engl.pdf?__blob=publicationFile&v=6; "De Maizière plant neue Behörde für Überwachung," *Computerwoche,* June 24, 2016, http://www.computerwoche.de/a/de-maiziere-plant-neue-behoerde-fuer-ueberwachung,3312792.

71 See Kahn, " 'snooper's Charter' Bill," and Severson, "Encryption Legislation Advances in France."

72 Paul Rosenzweig, "iPhones, the FBI, and Going Dark," *Lawfare* (blog), August 4, 2015, https://www.lawfareblog.com/iphones-fbi-and-going-dark.

73 See Australian Department of Defence, "iPhones and iPads now certified for classified government use," news release, March 30, 2012, http://news.defence.gov.au/2012/03/30/iphones-and-ipads-now-certified-for-classified-government-use/.

74 Ron Wyden, "This Isn't about One iPhone. It's About Millions of Them," *Backchannel,* February 19, 2016, https://backchannel.com/this-isn-t-about-one-iphone-it-s-about-millions-of-them-3958bc619ea4#.dltm7ruqi.

75 See Tait, "James Comey's Technical Challenge."

76 See Hennessey, "Encryption Legislation."

77 Apple, "Legal Process Guidelines: U.S. Law Enforcement," September 29, 2015, 9, http://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf.

78 See Greg Nojeim, "MLAT Reform Proposal: Protecting Metadata," *Lawfare* (blog), December 10, 2015, https://www.lawfareblog.com/mlat-reform-proposal-protecting-metadata.

79 See Spencer Ackerman, "Apple encryption case risks influencing Russia and China, privacy experts say," *The Guardian,* February 17, 2016, https://www.theguardian.com/technology/2016/feb/17/apple-fbi-encryption-san-bernardino-russia-china.

80 See Mozur and Perlez, "China Quietly Targets U.S. Tech Companies in Security Reviews."

81 See H.R. 4651, 114th Cong., 2d Sess. (2016), https://homeland.house.gov/wp-content/uploads/2016/03/2016.03.03_HR-4651-Commission.pdf.

82 Andrei Soldatov and Irina Borogan, "Putin Trolls Facebook," *Foreign Affairs,* November 3, 2015, https://www.foreignaffairs.com/articles/russian-federation/2015-11-03/putin-trolls-facebook.

83 Sergei Blagov, "Russia's 2016 Data Localization Audit Plan Released," Bloomberg, January 13, 2016 ("Roscomnadzor's regional department for Central Russia plans to audit Microsoft Corp. in March, McDonald's Corp. in May-July, Hewlett-Packard in August and Citibank N.A. in September–November").

84 Patrick H. O'Neill, "Russian bill requires encryption backdoors in all messenger apps," *The Daily Dot,* June 20, 2016, http://www.dailydot.com/layer8/encryption-backdoor-russia-fsb/; Matthew Bodner, "What Russia's New Draconian Data Laws Mean for Users," *The Moscow Times,* July 12, 2016, https://themoscowtimes.com/articles/what-russias-new-draconian-data-laws-mean-for-users-54552.

85 Cf. Justin Lynch, "The Tragedy of Ethiopia's Internet," *Motherboard,* February 1, 2016, https://motherboard.vice.com/read/the-tragedy-of-ethiopias-internet (describing Ethiopia's pervasive Internet surveillance and repression of journalists).

86 See Ellen Nakashima and Andrea Peterson, "Obama administration opts not to force firms to decrypt data—for now," *Washington Post,* October 8, 2015, https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html; see also http://apps.washingtonpost.com/g/documents/national/read-the-nsc-draft-options-paper-on-strategic-approaches-to-encryption/1742/ (NSC decision memorandum outlining options).

87 See generally George Friedman, "Taking the Strategic Intelligence Model to Moscow," *Geopolitical Weekly,* December 2, 2014, https://www.stratfor.com/weekly/taking-strategic-intelligence-model-moscow.

88 See Benjamin Wittes, "Leading From Behind on Encryption," Hoover Institution, Beyond Privacy and Security series paper (forthcoming 2016) (draft on file with author).

89 Ibid.

90 Hennessey, "Encryption Legislation" (emphasis added).

91 Harold Abelson, et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications," July 6, 2015, 10, https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf; Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair: How some extremely smart hackers pulled off the most audacious cell-network break-in ever," *IEEE Spectrum,* June 29, 2007, http://spectrum.ieee.org/telecom/security/the-athens-affair ("Basically, the hackers broke into a telephone network and subverted its built-in wiretapping features for their own purposes").

92 Cf., e.g., Stewart A. Baker, "Deposing Tim Cook," *Lawfare* (blog), February 27, 2016, https://www.lawfareblog.com/deposing-tim-cook (noting that iPhones for the Chinese market incorporate Chinese government-mandated WAPI security protocol for wireless networks).

93 H.R. 4651, 114th Cong., 2d Sess. (2016), https://homeland.house.gov/wp-content/uploads/2016/03/2016.03.03_HR-4651-Commission.pdf.

94 "Hillary Clinton's Initiative on Technology & Innovation."

95 See Brendan Sasso, "The Hill's Newest Encryption Fight—Over Committee Turf," *National Journal,* March 23, 2016, http://www.govexec.com/oversight/2016/03/hills-newest-encryption-fight-over-committee-turf/126895/ (" 'I think the chairmen and ranking members of the two committees of jurisdiction did not feel comfortable punting on it, in their opinion, by going with the commission,' " said Republican Rep. Darrell Issa).

96 Ellen Nakashima and Andrea Peterson, "Obama faces growing momentum to support widespread encryption," *Washington Post,* September 16, 2015, https://www.washingtonpost.com/world/national-security/tech-trade-agencies-push-to-disavow-law-requiring-decryption-of-phones/2015/09/16/1fca5f72-5adf-11e5-b38e-06883aacba64_story.html.

The preferred citation for this publication is:
Adam Klein, "Decryption Mandates and Global Internet Freedom," Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1608 (September 26, 2016), available at https://lawfareblog.com/decryption-mandates-and-global-internet-freedom.

About the Author

ADAM I. KLEIN

Adam Klein is a Visiting Fellow at the Center for a New American Security and a Council on Foreign Relations International Affairs Fellow. His research at CNAS focuses on the intersection of national security policy, technology, and law.

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 cybersecurity, 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

HOOVER INSTITUTION