A HOOVER INSTITUTION ESSAY

The International Legal Dynamics of Encryption

ASHLEY DEEKS

Series Paper No. 1609

There is a long and growing list of technologies that can be used for significant good or significant ill. These include the Internet, electronic banking, social media, and commercial drones. Add encryption to that list. The widespread use of end-to-end encryption—particularly when manufacturers set it as the default—offers significant foreign policy and national security benefits but also imposes costs. As a result, the US government writ large—and individual government agencies with diverse mandates—have had a difficult time weighing the overall costs and benefits of end-to-end encryption on the one hand and of mandated third-party access on the other.[1] In a leaked draft options paper, US officials involved in commerce, diplomacy, trade, and technology advocated for the president to "strongly disavow" a legislative mandate requiring technology companies to provide law enforcement access to encrypted communications.[2] The FBI, in contrast, argues that the growing inability of companies to decrypt communications, even pursuant to a court order, poses a very serious problem for law enforcement.[3] For now, the US government seems to have decided not to decide anything, at least publicly.

As difficult as it is to assess how to balance domestic equities when evaluating end-to-end encryption, it becomes exponentially harder when the debate shifts to the international plane. Anticipating reactions by like-minded and not-so-like-minded foreign governments, foreign encryption developers, corporations, and private actors who use encryption for purposes as diverse as dissident activities and terrorism is a multidimensional game, though with real stakes. To date, there has been little coordinated action on the international plane to address encryption,[4] though the possibility surely exists and interest in the topic has begun to build. If international discussions occur, what will they look like, in what forums might they take place, and on what aspects of encryption will they focus?

One way to begin to sort through the costs and benefits of promoting end-to-end encryption in the international context (or managing its proliferation) is to tease apart the interests of different actors within and across states. It is possible to treat encryption as predominantly a rights question, a law enforcement question, an intelligence question, an economic question, or an export control question.[5] Encryption obviously implicates all five interests at once. But placing any one legal paradigm in dominant focus makes it simpler to forecast the international dynamic on encryption within that paradigm.

The political power of the players who operate in and drive each paradigm matters. The stronger the players in the paradigm, the more likely it is that states developing their

encryption policies will give weight to that paradigm's preferred outcome over another. The paradigm one emphasizes also naturally affects which players within a given state will take the lead on international discussions. As discussed below, encryption discussions may arise in international forums as diverse as the Human Rights Council and trans-Atlantic trade negotiations. The international forum in which a conversation about encryption occurs may have an important impact on which views dominate.[6] It is therefore critical for the US government to decide as soon as possible which paradigms are most important to it and to plan for coordinated approaches across any international processes that arise.

This paper examines encryption through each of the five frames of reference. It first summarizes the particular frame's general perspective on end-to-end encryption. Then it evaluates the current views of relevant US actors in the framework, including both government officials and private actors. Finally, it describes international discussions (if any) that already have transpired within the given framework, considers existing models for future encryption discussions that might arise in that framework, and identifies some factors that may drive the outcomes in that framework. These forecasts are necessarily speculative, given that many states continue domestically to struggle to decide their positions on encryption.

The paper makes several points. First, there has been little discussion to date about encryption in international forums, though that may change as domestic debates about encryption are resolved. Second, the United States has stronger reasons to tolerate, or even to support, end-to-end encryption than do several other states that will be active players in encryption policy discussions. In light of the current US intelligence advantage relative to other states in obtaining access to encrypted information (whether through decryption or by taking advantage of vulnerabilities), and in view of the significant advantages of end-to-end encryption in the US corporate and privacy frames, the United States should be content to either affirmatively advance or passively allow end-to-end encryption as the preferred posture in the international arena. Third, the United States has ample opportunities to shape international discussions about encryption, even though some key actors (such as Russia, China, and France) are unlikely to be directly swayed by US arguments. The sooner that the United States establishes its position domestically, the sooner it will be able to exercise influence internationally and help shape the terms and outcome of the debates that transpire there.

A final introductory note: It is important to make a distinction between the type of encryption that governments use to protect their own information and the type of encryption that they allow their citizens to use (or forbid them from using). With regard to state use of encryption, states will generally be unable to prevent other states from accessing and using end-to-end encryption.[7] Indeed, the dominant position among states will be to obtain and use the strongest encryption possible on their government communications. As a result, this paper focuses on the access and use of end-to-end encryption by private actors, including in both business and personal exchanges.

Encryption as a human rights issue

Background

Foreign and domestic privacy advocates, international human rights lawyers, and civil liberties groups are among those who view end-to-end encryption first and foremost as a human rights issue. Those who operate within this paradigm almost universally advocate for widespread access to and use of end-to-end encryption. In international law terms, the idea is that encryption advances individual privacy and freedom of expression, two rights contained in the International Covenant on Civil and Political Rights (ICCPR). Encryption allows people to exchange ideas securely, without fear of government sanction.

Encryption has not yet been a topic of discussion in the UN General Assembly. However, David Kaye, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, recently produced a report about the role of encryption in human rights protection.[8] He argues:

> Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments.[9]

His report recognizes that states may impose legitimate restrictions on encryption, but he argues that those restrictions "must meet the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds (as set out in article 19 (3) of the Covenant); and must conform to the strict tests of necessity and proportionality."[10] He concludes that outright prohibitions on the use of encryption would be disproportionate because they would affect many people who use encryption for lawful ends.[11] He also asserts that requiring back-door access to encrypted data would be disproportionate because its impact would be widespread and indiscriminate.[12]

Kaye recommends, "States should adopt policies of non-restriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective, [and] require court orders for any specific limitation."[13] In practice, this recommendation would tend to preclude states from mandating that corporations provide mandatory third-party access, because doing so requires technical choices that would affect all users, not just users in specific cases.[14] Indeed, it is the very conundrum of how to gain access to encrypted information in limited, case-specific situations, with court authorization, that has so perplexed the US government and the technical community. In any event, Kaye's conclusions have garnered support from many international human rights advocates.[15]

Rendering legitimate law enforcement investigations more difficult can impose costs not only on the victims of crimes, but also on the human rights and well-being of large groups within a state (as in a hypothetical case in which an individual who commits a terrorist act remains at large within that state because law enforcement cannot obtain access to communications that would serve as evidence). That is, the use of encryption can be human rights-enhancing when it allows individuals to evade unlawful surveillance by lawless states, but does not necessarily enhance human rights when it allows individuals engaged in criminal acts to evade lawful surveillance in states attuned to the rule of law. But the predominant view of human rights and civil liberties groups appears to be that the latter situations are infrequent, or at least that the overall protection of individuals' communications is, on balance, more important than the ability to obtain electronic evidence in discrete criminal cases.[16]

US perspective

In the United States, the Department of State (including the Bureau of Democracy, Human Rights, and Labor) has the lead for the US government in advocating for and facilitating rights protections overseas and in advancing the use of the Internet to promote freedom and civic engagement abroad. In 2010, the then secretary of state Hillary Clinton announced that the State Department wanted to support "the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship"[17] or, more colloquially, to "help activists get around censorship and communicate without being nabbed by authorities."[18] The US government funded the development of a sophisticated encryption algorithm now used by WhatsApp, an application that many people around the world employ to communicate securely.[19] During the Arab Spring, the State Department provided political protesters with encryption tools that helped protect their anonymity.[20]

The Clinton State Department was not the first US government actor to advance the idea that encryption could promote human rights. In 1999, Representative Chris Cox (R-CA) argued, "America's companies, the leaders in encryption technology, must be able to export their products to China and around the world. Strong encryption is—as Beijing's communist leadership is well aware—a massive threat to totalitarian regimes and their government-maintained monopoly on information, because it permits individuals to communicate privately without fear of government eavesdropping or interception."[21] Fifteen years later, this posture appears to reflect the State Department's current views on encryption.

The substantive posture of the US government in the rights frame is not very different from that of human rights groups such as Human Rights Watch, which spearheaded support for David Kaye's recommendations. In the US submission to Kaye's call for information, it noted, "[T]he United States firmly supports the development and robust adoption of strong encryption . . . . Encryption . . . [is] especially important in sensitive contexts where

attribution could have negative political, social or personal consequences."[22] One potential difference is that the United States will be loath to accept *legal* arguments for encryption that rely on the view that the rights to privacy and freedom of expression impose obligations on states in their activities extraterritorially.[23] As a matter of *policy,* however, the US government's human rights advocates see encryption as an important way to advance the cause of democracy in states that are repressive or autocratic.

International forecast

What is likely to transpire on the international plane from a rights perspective? How will states manage calls by pro-privacy actors to permit all citizens to use end-to-end encryption? If states choose to let discussions proceed in this framework, options include a new treaty, a soft-law instrument, or public statements by supportive governments.

It seems very unlikely that any state would advocate for a new multilateral treaty on encryption, because the topic is relatively narrow and because many take the view that the rights that encryption protects already are enshrined in existing treaties such as the ICCPR. As with many human rights treaty negotiations, there is also the danger that certain states will push to weaken existing standards, rather than agree to apply the existing standards such as those in the ICCPR to new technology.

Assuming adequate support for end-to-end encryption, far more likely is a soft-law instrument that promotes end-to-end encryption and condemns those states that mandate (in opponents' words) "back doors" or (as FBI Director James Comey puts it) "lawful intercept capabilities."[24] A possible model here is the 2013 UN General Assembly Resolution entitled, "The Right to Privacy in the Digital Age."[25] That resolution affirmed that people have the same rights online that they have offline, including the right to privacy.

The Right to Privacy resolution was adopted by consensus.[26] Any resolution regarding end-to-end encryption, which could draw from the Special Rapporteur's recommendations on encryption, surely would not be. Indeed, it remains unclear whether the majority of the General Assembly would support the proposition that states should allow end-to-end encryption and resist mandating third-party access. In light of the states that currently ban or regulate the use of end-to-end encryption—such as Russia, Pakistan, and Colombia—we might be skeptical that sufficient support currently exists for a resolution like this.[27] It is possible that the United States, if it chose to commit to this approach, might be able to rally sufficient support for a pro-encryption resolution, with the backing of states such as Germany and the Netherlands. In any case, the Human Rights Council seems poised to continue to discuss issues related to privacy and online freedom of expression.[28]

Barring a US push to conclude a resolution, the United States and a group of like-minded states could issue coordinated public statements that articulate the human rights

advantages of end-to-end encryption. A German think tank has proposed this approach, arguing that the United States and Germany should take a unified approach to favoring end-to-end encryption.[29] As discussed below, this may be a normatively appealing approach because US commercial and intelligence interests (including technologists' interests in Internet security and stability) ultimately pull in the direction of end-to-end encryption too.

Encryption as a law enforcement issue

Background

Law enforcement equities are a key policy driver in the encryption debate. Viewed as a law enforcement issue, end-to-end encryption poses a problem. There is an ongoing and intense debate about how serious a problem it is, but most commentators concede that the inability of law enforcement to access certain private communications pursuant to a court order harms its ability to investigate and prosecute crimes.[30] Therefore, those who come to the encryption issue from a law enforcement perspective seek to ensure that manufacturers build into their products mandated third-party access. Where service providers hold data in the cloud, this might include requiring service providers to retain the encryption key. Where data are held on an individual's device, this could include requiring users to escrow their private keys.[31] Various reports have decried this and other proposed solutions as introducing significant risk into secure systems,[32] while others have offered proposals that they believe would not pose significant security risks.[33]

Around the world, more governments are either demanding third-party access to encryption systems or banning encryption services outright, according to Freedom House's 2015 "Freedom on the Net" report.[34] Amnesty International reports, "Several countries already limit who can encrypt their communication or the strength of encryption allowed, such as Cuba, Pakistan and India. Others, such as Russia, Morocco, Kazakhstan, Pakistan and Colombia, sometimes go as far as banning it altogether."[35]

Though the reasons for these bans or restrictions vary, some states have implemented these rules for law enforcement reasons. For example, several states require providers to turn over encryption keys to the government in the context of criminal investigations.[36] China requires companies to provide technical support for decryption, although it has not demanded that companies turn over encryption keys.[37] Its new antiterrorism law requires companies to release "technical interfaces" and to "assist with decryption should security agencies deem it necessary to avert or investigate a terrorist attack."[38] France imposes criminal sanctions if a person refuses to turn over to authorities a known decryption key for an encryption standard where an actor used encryption to facilitate or commit a crime.[39] France is having an ongoing debate about new laws that would force companies to decrypt communications in terrorism investigations.[40]

The United Kingdom likewise is debating the Investigatory Powers Bill, which includes provisions related to encryption. The bill states that the secretary of state may serve a "technical capability notice" on a telecommunication service provider to facilitate assistance with authorizations under the bill, but may only do so where he or she determines that "it is (and remains) practicable for those relevant operators to comply with those requirements."[41] This could include obligations "relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data."[42] An accompanying fact sheet states, "This provision will replace the current obligation to maintain a permanent interception capability and will provide a clear basis in law for CSPs to maintain infrastructure and facilities to give effect to interception and other warrants."[43] The UK government has stated that the bill would not require companies to incorporate third-party access, but only would require companies to remove encryption that they themselves have applied to a communication.[44]

In sum, states have taken a variety of domestic approaches to encryption to address their perceived law enforcement needs, but there have been no public efforts to harmonize these requirements in a multilateral context.

US perspective

The main US players in this frame are the Department of Justice, the FBI, and state and local law enforcement officials. US law enforcement interests are generally consistent with those of other states, although the United States is more committed than some other states to ensuring access by governments only pursuant to lawful process, which often requires court orders. Further, like the US intelligence community, US law enforcement recognizes a real value to end-to-end encryption, which guards US citizens and corporations against various types of hacking and cybercrime.[45]

To date, the US administration has not sought legislation to address the "going dark" problem, although Senators Dianne Feinstein (D-CA) and Richard Burr (R-NC) have proposed legislation to achieve that goal. Their draft bill would require providers of communications services and products, if presented with a lawful order, to provide information in an intelligible format or provide the necessary technical assistance to make the data intelligible if the data were made unintelligible by a feature that the company created.[46] Many commentators have criticized the bill, and the US government has declined to endorse it.[47]

As discussed below ("Encryption as an intelligence issue"), in some (although surely not all) truly critical situations, the National Security Agency (NSA) might be able to help law enforcement gain access to encrypted communications. However, such assistance may reveal vulnerabilities that the manufacturer would fix (to the detriment of future exploitation by the US intelligence community), and law enforcement might not be able to

use the accessed communications in a criminal prosecution.[48] This makes the widespread use of end-to-end encryption marginally less troubling, but it still undoubtedly complicates the law enforcement mission.

International forecast

There has been limited public discussion among states about encryption from a law enforcement perspective, although states such as the United States and United Kingdom surely have conferred privately about the topic.[49] States might seek to harmonize their law enforcement approaches to encryption for two reasons. First, harmonizing the demands placed by several democratic states on communications providers might put those states in a stronger position to persuade the providers to cooperate voluntarily. (The providers might prefer, on balance, to provide one type of third-party access to states' law enforcement than have to navigate a panoply of access requirements.) Second, states that undertake extensive law enforcement cooperation with each other would prefer to see their international law enforcement partners be able to produce more evidence in response to legal assistance requests, something extraordinary access would facilitate. Neither of these reasons clearly necessitates that states harmonize their law enforcement approaches to encryption, however, and it remains very possible that international law enforcement cooperation on encryption issues will never transpire, at least directly.

If states chose to let their law enforcement officials take the lead in sorting out how to approach encryption, these officials presumably would seek an international arrangement that would require each state-party to ensure that its telecommunications and Internet companies design products that permit mandated third-party access pursuant to transparent legal requirements such as a judicial warrant. The officials might also clarify that existing mutual legal assistance treaties could serve as an appropriate mechanism by which to obtain decrypted information for criminal investigations; or they might establish expedited data access arrangements such as the one that the United States and United Kingdom currently are negotiating.[50] The arrangement also presumably would prohibit individuals from employing end-to-end encryption in their communications, though one could imagine that, if technologically feasible, states would create carve-outs for industry sectors such as critical infrastructure, banking, and the like.

In light of US and European concerns about the misuse by states such as China and Russia of mandated third-party access, the United States and European states might want to pursue this type of arrangement only among a "trusted circle" of states. However, as some have postulated, other states would be quick to adopt their own versions of mandated third-party access, and US and European corporations would have a hard time resisting such mandates if they wanted to sell inside those other states.[51]

Persuading a "trusted circle" to adopt this law enforcement framework—assuming this were the route that the United States chose—would be difficult because states like Germany and

the Netherlands already have indicated that they are committed to end-to-end encryption. Having credible countries stay outside the "trusted circle" might push certain corporations to relocate to those "end-to-end encryption" countries. States that allow their companies to manufacture end-to-end encryption products will take some business away from those that do not. How large that shift would be is unknown. Also unknown is how many people would make the effort to obtain illicit end-to-end encryption applications.[52]

If states' law enforcement officials sought in a limited multilateral forum to regulate end-to-end encryption and to demand third-party access, it is unclear what international models they might draw from. None of the existing formats used by states to promote international criminal or law enforcement cooperation is well-suited to this goal. There are two basic categories of international law related to criminal issues: treaties that facilitate transnational law enforcement cooperation (such as mutual legal assistance treaties) and treaties that require states to criminalize certain actions (such as acts of terrorism or genocide). Mutual legal assistance treaties often are bilateral, and would remain as a tool by which states could obtain decrypted information from each other. But they would not on their own be a helpful model for the arrangement discussed above.

Nor does it seem likely or useful for states collectively to agree to criminalize particular facets of encryption use. Some states might choose unilaterally to criminalize the use of encryption to conceal, plan, or conduct crimes, but those provisions might duplicate existing "aiding and abetting" provisions, and there is little need for international agreement to criminalize such acts. The fact that there is no obvious international criminal law model to which states might turn does not mean that states could not create a new model. But the fact that nothing comparable exists illustrates that encryption has raised a problem with unique features.

Encryption as an intelligence issue

Background

If one views encryption primarily as an intelligence issue, it quickly becomes clear that states' intelligence agencies are internally conflicted about end-to-end encryption because of their multiple missions. One mission is to collect and analyze intelligence, including the communications of foreign nationals. In this mode, intelligence agencies favor weak or no encryption, because that enables their collection and analysis mission. Another mission, however, is an "information assurance" mission: actors such as the NSA and the UK Government Communications Headquarters (GCHQ) are responsible for securing both governmental and certain private sector data and communications.[53] As the head of GCHQ put it, "Information assurance is at the heart of everything we do. And I am accountable to our prime minister just as much, if not more, for the state of cyber security in the UK as I am for intelligence collection."[54] Information assurance missions are facilitated by the use of end-to-end encryption, which protects systems against data interception. Intelligence agencies themselves thus gain and lose from end-to-end encryption.

Some intelligence agencies will emphasize another angle as well: their perceived need to monitor their own citizens' communications. States such as Russia and China exercise quite strict control over their citizens' electronic communications, including by blocking the use of encrypted virtual private networks that allow individuals to browse the web anonymously.[55] Thus, while these states surely seek to employ the strongest possible encryption for their own communications, they limit their citizens' ability to use end-to-end encryption. As a result, they are able more easily to monitor their citizens' communications, including those of dissenters and human rights groups.[56]

Other states have taken a different approach to their citizens' use of end-to-end encryption. States such as Germany (and possibly the Netherlands) favor end-to-end encryption, in part because they are worried about the ability of the Five Eyes countries (the United States, United Kingdom, Canada, Australia, and New Zealand) to collect the electronic communications of their citizens.[57] For intelligence services like Germany's, "information assurance" values thus appear—at least for now, and at least publicly—to trump collection values.

Different sets of states face varying degrees of public pressure to support end-to-end encryption. Strong democracies (and, correspondingly, their intelligence services) are facing significant pressure from citizens, corporations, and others to promote end-to-end encryption. But autocracies and weak democracies that worry about their own survival often have powerful and opaque intelligence services, tend to disfavor end-to-end encryption, and face less overt domestic condemnation for doing so.

US perspective

The key intelligence player for the United States in the encryption space is the NSA. As noted above, the NSA has both information assurances and electronic surveillance responsibilities, and therefore has mixed views on end-to-end encryption. Some US intelligence officials have expressed strong concern about how encryption complicates intelligence collection. For instance, CIA Director John Brennan stated, "[T]here are a lot of technological capabilities that are available right now that make it exceptionally difficult both technically as well as legally for intelligence security services to have the insight they need to uncover [terrorist networks and activities]."[58]

These comments are counterbalanced by the statements of other current and former intelligence officials who have come out in favor of end-to-end encryption. Most notably, NSA Director Admiral Michael Rogers has argued that "[e]ncryption is foundational to the future" and that it is a waste of time to try to eliminate it.[59] Rogers's predecessor, General Michael Hayden, has argued that end-to-end encryption is "good for America,"[60] and former secretary of homeland security Michael Chertoff said he believes that "end-to-end encryption of data with only the sender and intended recipient possessing decryption keys" advances the greater public good.[61]

What should we make of these pro-encryption comments by current and former US intelligence officials? Two factors likely are in play. First, these officials are placing significant weight on the NSA's information assurance responsibilities and making a broader calculation about the advantages of end-to-end encryption for individuals and corporations (through the other lenses discussed in this paper). As a former Federal Trade Commission official put it, "Support for encryption is high among officials tasked with addressing the threat that state-sponsored hackers pose to the country's private networks, such as those in the intelligence community."[62]

Second, these officials are particularly well-suited to understand NSA's decryption and related capabilities, and presumably are taking into account their background knowledge about those capabilities in making their pro-encryption statements. Specifically, it seems fair to assume that the NSA has the strongest hacking and decryption capabilities in the world.[63] The NSA also presumably has—for now, at least—the strongest ability to develop new capabilities to respond to new challenges. Indeed, in an Op-Ed column, Hayden and Chertoff (both of whom now work in the private sector and may have slightly different interests from current US officials) concluded that "[i]f law enforcement and intelligence organizations face a future without assured access to encrypted communications, they will develop technologies and techniques to meet their legitimate mission goals."[64] This means that even if end-to-end encryption becomes ubiquitous, the NSA is likely to retain or develop abilities to penetrate many of those communications, whether through decryption or by exploiting vulnerabilities before the sender encrypts the information or after the recipient decrypts it. This is not to suggest that doing so will be easy or inexpensive, or that the NSA will be able to crack all encrypted communications, but it suggests that end-to-end encryption is not fatal to the US intelligence collection mission.

As a related matter, strong NSA capabilities suggest that the US law enforcement case against encryption might be overstated, at least in very serious criminal cases. There are costs to revealing particular vulnerabilities in products, and the NSA may be reluctant to sacrifice the advantages it gains from a vulnerability for access to data in a single case.[65] But there may be some set of cases in which the NSA can covertly crack an encrypted phone and provide the Department of Justice with the information, thus giving the DOJ a lead that allows it to obtain alternative evidence that it could use in the case without revealing sources and methods.

Finally, the NSA currently has two additional intelligence advantages over other states: it can work in concert with US companies that sell their products overseas, and it can more easily obtain metadata from US companies.[66] From the NSA's perspective, it is better to have foreign users use US phones (even if they contain default encryption) than to have them shift to products manufactured by foreign companies, which are located outside the United States and which are less likely to have a good relationship with the NSA. As a Chertoff Group report put it, "By driving actors away from American products and systems we might

have the perverse effect of driving internet traffic and technology companies offshore, depriving our analysts of valuable metadata information."[67]

International developments

In the intelligence frame, we are very unlikely to see international discussions that seek to mandate either end-to-end encryption on the one hand or third-party access on the other. The primary reason for this is that we rarely see *any* kinds of public international discussions in the intelligence frame.

As I have written elsewhere, there are a number of reasons why states have rarely developed international rules to regulate intelligence.[68] First, intelligence collection implicates a state's core equities.[69] Here, the use in one state of end-to-end encryption by the government itself and by the state's citizens makes it more difficult for foreign states to spy on that state and its citizens. So no state will agree to regulate its own use of encryption, and all states will be loath to consent to rules that constrain how they regulate their own citizens' use of end-to-end encryption.

Second, a state's ability to penetrate or circumvent end-to-end encryption is something it would seek to hold secret. This means that from an intelligence perspective, states would prefer to say as little as possible about encryption for fear of disclosing capabilities. A state that is very capable, such as the United States, gains a comparative advantage if citizens worldwide use end-to-end encryption, because it is more likely to be able to access those communications (including those of foreign citizens) than other states are to be able to access US government and private communications. However, the United States will (and should) be loath to discuss its capabilities in a multilateral setting. Relatedly, states with strong expertise in intelligence collection, including through electronic surveillance, decryption, and hacking, will have few reasons to *want* to have encryption or decryption regulated.

Even if states were inclined to discuss the intelligence aspects of end-to-end encryption in a multilateral forum, consensus would be difficult to achieve because states currently have divergent views about the relative merits of end-to-end encryption. As discussed above, weak encryption or third-party access helps intelligence services, including the NSA, engage in offensive intelligence collection overseas. Indeed, some parts of the NSA might prefer that foreign states such as Russia prohibit their citizens from using end-to-end encryption or require companies doing business in those states to design third-party access because it makes NSA's collection job easier.[70] At the same time, in view of its information assurance mission, NSA would not want to sign onto a multilateral framework that *required* all states to mandate third-party access.

In a world in which states (including America) are constantly trying to outperform state and nonstate enemies on the intelligence collection and counter-espionage fronts,

we should not expect to see any kind of widespread international discussion, let alone agreement, regarding the use by intelligence services of end-to-end encryption or mandated extraordinary access. The only type of international discussion that might occur in this context is among the Five Eyes nations, which may already share some sensitive set of decryption or other data acquisition techniques. This could produce modest benefits for the United States in both the intelligence and law enforcement contexts, if a lead from decrypted information by another Five Eyes state helps the United States respond to, say, a terrorist attack.

In short, in view of its comparative advantage, the United States should be content from an intelligence perspective if there is no agreement on the international front in any of the frames discussed above—or even if one of the other frames produces an outcome favoring end-to-end encryption. One important caution is warranted, however: an intelligence approach that "favors" end-to-end encryption is strongly hypocritical, if the reason for favoring end-to-end encryption is that the United States believes that it can still capture much of the encrypted information. That said, the United States surely will continue to try to keep secret as many of its capabilities as possible. A certain level of cynicism and skepticism will continue to attach to NSA activities, no matter what the NSA does or does not do.

Encryption as a commercial or free trade issue

Background

Privacy, law enforcement, and intelligence are not the only lenses through which one can view encryption. Some actors—including, in particular, corporations—see end-to-end encryption as a commercial or free trade issue. Those who view encryption primarily through this lens tend to support end-to-end encryption and object to state-imposed requirements on companies to build or import only those products that allow third-party access.[71] These actors are driven primarily by profit motives and a need to maximize value for their shareholders, though they may also have a discrete pro-privacy commitment. They believe that their customers desire the privacy protections that accompany end-to-end encryption and that fewer restrictions by foreign governments on the import of encryption technology mean larger markets in which to sell their goods.[72] It is possible, of course, that if consumers begin to demand that these companies engage in more cooperation with governments, profit motives might drive corporate policies in a different direction.

For now, however, US companies, the most powerful drivers in this space, favor and promote end-to-end encryption.[73] For example, in 2015, two industry associations for major software and hardware companies (including Apple, Google, Facebook, IBM, and Microsoft) wrote a letter to the Obama administration making clear that they opposed "any policy actions or measures that would undermine encryption as an available and effective tool."[74] The industry groups argued that online commerce has flourished because consumers believe

their payment information will be secure.[75] They wrote, "Consumer trust in digital products and services is an essential component enabling continued economic growth of the online marketplace. . . . Accordingly, we urge you not to pursue any policy or proposal that would require or encourage companies to weaken these technologies, including the weakening of encryption or creating encryption 'work-arounds.' "[76]

There is some debate about the extent to which individuals purchase or use products and services because of their security features, rather than because of their ease of use or attractiveness of design.[77] Nevertheless, companies such as Apple and Facebook (which owns WhatsApp) seem persuaded that a strong pro-encryption posture is integral to their corporate models. Indeed, the Department of Justice argued that Apple's resistance to unlocking the San Bernardino shooter's iPhone, "despite the technical feasibility of doing so, instead appears to be based on its concern for its business model and public brand marketing strategy."[78] In short, companies that produce products incorporating encryption tend to favor the reduction or elimination of non-tariff barriers to trade in such products.

US perspective

Because US companies are the most active players in commercial encryption, the US perspective tracks (and indeed drives) the generic corporate views on end-to-end encryption just described. The most powerful US companies in this space—Apple, Google, Yahoo, Dropbox, Microsoft, and Twitter—do business both inside the United States and overseas.[79] Within the US government, the Commerce Department and the Office of the US Trade Representative have the lead on advancing US commercial interests abroad.

From the commercial perspective, the United States would like to reduce trade barriers for these companies, which means helping them avoid excessive regulation by foreign (importing) states. As FBI Director Comey noted in a recent speech, "It is also true that other countries—particularly those without our commitment to the rule of law—are using this debate [on encryption] as a cynical means to create trade barriers [and] impose undue burdens on our companies."[80]

If the United States chose to act with US commercial interests foremost in mind, the United States would urge foreign states to allow imports of products that contain or facilitate the use of end-to-end encryption. US companies seek to use end-to-end encryption as a selling point for their products in major markets (such as Europe and China). The US government's posture itself becomes critical here: only if the United States itself does not require its companies to structure their products to permit third-party access could it be at least somewhat persuasive to urge China to allow the import and use of those products. US corporations undoubtedly would prefer to avoid having to incorporate different technical requirements in the same products when sold in different markets. Further, as the leaked

National Security Council memo notes, a US approach that favors end-to-end encryption may help companies sell their products because it makes it easier for the companies to persuade users that they are not facilitating NSA collection.[81]

International forecast

To date, international efforts to deal with end-to-end encryption as a commercial issue have manifested themselves in the form of trade treaties. For instance, the Trans-Pacific Partnership (TPP), a free trade agreement just concluded among a dozen states in North America, South America, Australia, and Asia, addresses encryption in its chapter on technical barriers to trade.[82] Parties to the TPP may not require manufacturers or suppliers to provide access to a commercial product's encryption technologies as a condition of manufacture, sale, or use.[83] The provision allows an exception to that rule when the sale is to a party's government.[84] The provision also states, "[T]his Section shall not be construed to prevent a Party's law enforcement authorities from requiring service suppliers using encryption they control to provide, pursuant to that Party's legal procedures, unencrypted communications."[85] In addition, the agreement contains a catchall national security provision that states, "Nothing in this Agreement shall be construed to . . . preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests."[86]

In short, the TPP protects companies from disclosing their commercial encryption technologies to foreign states unless they are selling the products to states themselves. It is not yet clear, however, the extent to which the TPP contemplates that states-parties may require third-party access for law enforcement purposes.[87] The annex language might not preclude the use of end-to-end encryption, though the national security catchall seems to leave open that a state-party could demand third-party access to protect "its own essential national security interests." This result presumably is only partly satisfactory to the companies that sell products or technologies containing encryption because it leaves significant ambiguity about what states-parties may require of them.

At a minimum, we should expect to see TPP-like provisions in future trade treaties such as the Transatlantic Trade and Investment Partnership (T-TIP), which the United States and the European Union currently are negotiating. US companies, as major producers of products using encryption, might even pressure the US government to try to dilute (or further clarify) the TPP language on law enforcement access in future agreements and to urge future treaty partners to eliminate non-tariff barriers to trade for commercial products containing end-to-end encryption. The likelihood that the United States could obtain this kind of concession from states such as the United Kingdom and France appears slim for now, though the United States might do so in certain bilateral trade treaties with states that support end-to-end encryption.

Encryption as an export control issue

Background

Whereas trade agreements govern how states-parties may regulate certain products coming into their territory, export control regimes regulate domestically what products a state's companies may export and what government approvals they must obtain before doing so. Before an encryption product even enters the transnational stream of commerce, its producer must meet domestic export requirements, which in some cases prohibit corporations from selling to purchasers in selected states.

States establish export controls for a variety of reasons, including as a means to advance national security and foreign policy goals. A variety of states regulate the export of cryptography to other states because they perceive that end-to-end encryption can pose a threat to their national security. In contrast, from a profit perspective, companies prefer to avoid having states place export controls on their products, so as to widen their markets.

Certain states have chosen to coordinate their export controls internationally. Forty-one states have joined the 1995 Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA).[88] Pursuant to the non-binding WA, states coordinate their export controls over both conventional arms and dual-use items (that is, items that have both military and civilian uses). The general idea is to prevent destabilizing accumulations or unauthorized transfers or re-transfers of selected items.

Before 1998, all encryption products other than mass market or public domain software were considered dual-use items in the WA framework.[89] The WA subsequently decontrolled items that do not use encryption primarily for computing, communicating information, networking, or information security purposes, and where the cryptographic functionality is limited to supporting the item's specific functions.[90]

Unlike the other four equities discussed above, international coordination of export controls is likely to follow, rather than drive, substantive decisions about encryption. Export controls are a tool by which to implement policy, rather than policy drivers themselves.

US perspective

Because the United States participates in WA, US export controls draw from and are consistent with WA. Currently, exports of end-to-end cryptography are regulated by the Commerce Department through the Export Administration Regulations.[91] From a US export control perspective, the US government presumably would like to avoid having end-to-end encryption make its way into the hands of hostile governments or private actors, and likely is content with the status quo. However, the importance of the export control regime hinges on how confident the United States is that its companies alone are the key source of very

sophisticated encryption. That is, if it is easy for disfavored states or private actors outside the United States to build or obtain high-level encryption from other sources, the need for a robust export control regime is diminished.

Experts seem to agree that the United States currently is the source of much high-level encryption, but they disagree about the extent to which non-US actors can provide comparable products. In a hearing before the Senate Intelligence Committee, CIA Director Brennan stated:

> US companies dominate the international market as far as encryption technologies that are available through these various apps, and I think we will continue to dominate them. So although you are right that there's the theoretical ability of foreign companies to be able to have those encryption capabilities that'll be available to others, I do believe that this country and this private sector is integral to addressing these issues.[92]

Bruce Schneier, who with colleagues conducted a worldwide survey of encryption products, concluded that while the United States produces the most products that use encryption, and while those products are widely used by companies and consumers, two-thirds of the total hardware or software products incorporating encryption are produced outside the United States.[93] Schneier noted, "Our survey demonstrates that such switching [away from a US encryption product] is easy. Anyone who wants to evade an encryption backdoor in US or UK encryption products has a wide variety of foreign products they can use instead."[94]

Here, the United States would do well to carefully assess reports such as Schneier's so as to be able correctly to assess the extent to which export controls on encryption continue to be important to US national security or have become too easily circumvented to make their retention worthwhile.

International forecast

Any changes to the international export control regime established in the Wassenaar Arrangement presumably would take place within that forum. If a number of states that participate in the WA reached the conclusion that end-to-end encryption was, on balance, beneficial to the global population, they would need to propose adjustments to the WA. Those adjustments might include the retention of export and re-transfer limits to certain states, though the more widely available end-to-end encryption is, the easier it will be for those "rogue" states to circumvent limits imposed by the WA.

If the United States chose instead to pursue an approach that entailed mandating third-party access—by requiring key escrow, for instance—it would need to consider whether to propose alterations to the WA. For example, if the United States chose to mandate domestically that corporations using encryption create a dual key escrow system by which

the corporations held one key and the government held another, the United States might want to try to use the WA to prevent non-democratic states from gaining access to that technology.[95] The fear is that some states would misuse the dual key system to gain access to citizens' communications without authorization from a court or other appropriate authority. Of course, non-democratic states could demand that their own companies or any companies doing business in their territory build in third-party access, regardless of WA limitations.

Conclusion

These are early days for international interactions among states on encryption. Where states have discussed encryption internationally, they have done so in modest contexts in which the need to harmonize standards is important to achieve a clear goal—as with trade and export controls. More robust multilateral discussions about encryption standards are, at this stage, still premature because states continue to develop their domestic positions. However, there are at least five frameworks in which encryption issues arise, and it is important for the United States to both determine its position on end-to-end encryption and prepare to coordinate that position across these frameworks. There is likely a modest first-mover advantage to be gained by deciding the US position quickly and promoting that position in all five frameworks.

One key question remains to which the answer is, for now, unknowable: If the United States pursues an end-to-end encryption approach or even a procedurally stringent third-party access approach, to what extent can it influence other states to follow? A possible source of lessons in this regard is the US approach to the use of targeted killings. The United States, recognizing that it is setting important international precedent in its use of this tool, has imposed on itself a large number of procedural rules and substantive standards to follow when conducting those killings. Will this evidence of US self-constraint have an effect on how other states (including Russia, China, and Israel) conduct similar killings in the future? Or will states such as Russia draw only on the larger legal conclusion—that the use of these killings is internationally lawful—and disregard the constraints built around them? Likewise, if the United States adopts a procedurally stringent third-party access requirement, will other states feel pressure to adopt similar self-constraints? One important difference is that, unlike self-imposed legal standards, the US imposition (or rejection) of a technical standard on US manufacturers has implications for many states that cannot (as a political or practical matter) bar the use of US products inside their own countries. American standard-setting in the encryption context thus is quite likely to have more tangible international effects than legal standard-setting in the drone context.

NOTES

1 I will refer to "end-to-end encryption" as an encryption system in which only the intended sender and recipient of the communication (whether different people at the same time, or the same person but at different times) can

decrypt the communication and that is not created to require government access by means such as escrowed encryption keys. I will refer to "mandated third-party access" as the ability to access the content of encrypted communications by law enforcement (or other government actors). I recognize that these are crude models, but I believe that they are sufficient for the points I hope to make herein.

2 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; "Read the NSC draft options paper on strategic approaches to encryption," *Washington Post,* http://apps.washingtonpost.com/g/documents/national/read-the-nsc-draft-options-paper-on-strategic-approaches-to-encryption/1742/.

3 See, e.g., James B. Comey, director, Federal Bureau of Investigation, joint statement with Deputy Attorney General Sally Quillian Yates before the Senate Judiciary Committee, "Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy," July 8, 2015, Washington, DC, https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy. See also Cyrus R. Vance Jr., François Molins, Adrian Leppard, and Javier Zaragoza, "When Phone Encryption Blocks Justice," *New York Times,* August 11, 2015, http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html (identifying law enforcement concerns of various countries). For a similar context in which actors within the US government have had difficulty establishing a legal and policy position, see "United States Faces Challenges in Addressing Global Cybersecurity and Governance," Government Accountability Office, July 2010 (discussing cyber operations); Matthew Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law* 36 (2011): 421, 436 ("[B]ecause the main bureaucratic actors have divergent policy priorities amid a rapidly evolving strategic environment, it probably has been and likely will remain difficult for the U.S. government to develop and articulate clear legal positions on what sorts of actions in cyberspace constitute illicit force").

4 The most comprehensive international effort to date to establish recommended encryption policies took place in the Organisation for Economic Co-operation and Development in 1997. The resolution and guidelines took into account the sometimes-competing privacy, commercial, national security, and law enforcement aspects of encryption, though the document was non-binding. See "Recommendation of the Council concerning Guidelines for Cryptography Policy," C(97)62/FINAL, March 27, 1997, http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=115&InstrumentPID=111&Lang=en&Book=False (recognizing that "due to the inherently global nature of information and communications networks, implementation of incompatible national policies will not meet the needs of individuals, business and governments and may create obstacles to economic co-operation and development; and, therefore, national policies may require international co-ordination").

5 Some might consider encryption to be first and foremost a network security issue. However, because there is no one international forum that will consider encryption from that perspective, and because several of these frameworks take into account network security equities, the paper does not treat network security in a stand-alone frame.

6 See Rebecca Ingber, "Interpretation Catalysts and Executive Branch Legal Decisionmaking," *Yale Journal of International Law* 38 (2013): 359 (illustrating how the entry point into the US government for a particular issue affects the substantive resolution of that issue).

7 They may try to limit each other's access by way of export controls, but that seems likely to have only a weak impact on access to end-to-end encryption by major state players in this space (including China, Russia, European Union member states, India, Brazil, and Japan).

8 David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," A/HRC/29/32, May 22, 2015. The UN Security Council's Counter-Terrorism Committee also has discussed encryption challenges but has not produced a written product on the topic. See David Fidler, "UN Counter-Terrorism Committee Tackles Terrorist Use of the Internet and Social Media," *Net Politics* (blog),

Council on Foreign Relations, February 4, 2016, http://blogs.cfr.org/cyber/2016/02/04/un-counter-terrorism-committee-tackles-terrorist-use-of-the-internet-and-social-media/.

9 Kaye, "Report," 5, note 9.

10 Ibid., 11.

11 Ibid., 14.

12 Ibid., 15.

13 Ibid., 19.

14 Amnesty International, "Encryption: A Matter of Human Rights," March 21, 2016, http://www.amnestyusa.org/research/reports/encryption-a-matter-of-human-rights. ("The briefing warns against attempts to make companies create a 'backdoor' in encryption software. It says these measures violate international human rights law, because they indiscriminately undermine the security of the communications and private data of anyone using the software.")

15 Human Rights Watch, "Promote Strong Encryption and Anonymity in the Digital Age," June 17, 2015, https://www.hrw.org/news/2015/06/17/promote-strong-encryption-and-anonymity-digital-age-0 (reflecting support by thirty civil society groups for Kaye's recommendations). Nor is this a new posture for civil liberties groups. In 1997, a large number of rights groups, including Human Rights Watch, issued a Member Statement on behalf of the Global Internet Liberty Campaign. The statement criticized a then-new UK encryption policy that would have required companies to provide government access to encrypted communications and concluded that "mandatory key recovery policies would make Britain a second-class nation in the Information Age." See Yaman Akdeniz, "Global Internet Liberty Campaign Member Statement," February 1998, http://www.cyber-rights.org/crypto/gilc-dti-statement-298.html.

16 See, e.g., Amnesty International, "Encryption."

17 Hillary Clinton, "Remarks on Internet Freedom," speech at Newseum, January 21, 2010, Washington, DC, http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

18 Elias Groll, "How Hillary Clinton Helped Build WhatsApp's State-of-the-Art Encryption," *Foreign Policy,* April 6, 2016, http://foreignpolicy.com/2016/04/06/how-hillary-clinton-helped-build-whatsapps-state-of-the-art-encryption/.

19 Ibid.

20 Chertoff Group, "The Ground Truth About Encryption And The Consequences of Extraordinary Access," 2016, 14.

21 Christopher Cox, "China: Export of Technology Would Be Liberating Force," *San Jose Mercury News,* March 27, 1999.

22 See letter from Permanent Representative of the United States to the United Nations and Other International Organizations in Geneva, to Special Rapporteur David Kaye, February 26, 2015, http://www.ohchr.org/Documents/Issues/Opinion/Communications/States/USA.pdf.

23 Reply of the Government of the United States of America to the Report of the Five UNCHR Special Rapporteurs on Detainees in Guantanamo Bay, Cuba, March 10, 2006, 4, http://www.state.gov/documents/organization/98969.pdf ("By its express terms and clear negotiating history, the International Covenant on Civil and Political Rights ['ICCPR'] applies to each State Party only with respect to 'individuals within its territory and subject to its jurisdiction' ").

24 FBI Director James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" speech at Brookings Institution, Washington, DC, October 16, 2014.

25 UN General Assembly resolution, "The Right to Privacy in the Digital Age," A/RES/68/167, December 2013.

26 UN News Centre, "General Assembly backs right to privacy in digital age," December 19, 2013, https://www.un.org/apps/news/story.asp?NewsID=46780.

27 Amnesty International, "Encryption."

28 A recent resolution on the "promotion, protection and enjoyment of human rights on the Internet" concluded by stating that the Human Rights Council "decides to continue its consideration of the promotion, protection and enjoyment of human rights, including the right to freedom of expression, on the Internet and other information and communication technology, as well as of how the Internet can be an important tool for fostering citizen and civil society participation . . . and for exercising human rights . . . ." A/HRC/32/L.20, June 27, 2016.

29 *Stiftung Neue Verantwortung,* "Transatlantic Digital Dialogue: Rebuilding Trust through Cooperative Reform," 2015, http://www.stiftung-nv.de/publikation/transatlantic-digital-dialogue-rebuilding-trust-through-cooperative-reform.

30 Compare Chertoff Group, "The Ground Truth About Encryption," 8 ("What little data there is suggests that encryption technology has, in fact, been an impediment to successful law enforcement but that the magnitude of that impediment is modest") with Comey, speech, "Going Dark."

31 Chertoff Group, "The Ground Truth About Encryption," 5; ibid., 14 (describing French legislative proposal to "require technology companies to configure their systems such that police and intelligence agencies could always access their data, effectively banning technology companies from providing strong endpoint encryption").

32 Chertoff Group, "The Ground Truth About Encryption," 2; "Don't Panic: Making Progress on the "Going Dark" Debate," Berkman Center for Internet & Society at Harvard University, February 1, 2016, https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf; Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity* 1, no. 1 (November 17, 2015); "Going Dark Going Forward: A Primer on the Encryption Debate," House Homeland Security Committee, June 2016, https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf.

33 See, e.g., Matt Tait, "An Approach to James Comey's Technical Challenge," *Lawfare* (blog), April 27, 2016, https://www.lawfareblog.com/approach-james-comeys-technical-challenge (describing a "cryptographic envelope" two-key proposal).

34 Groll, "What'sApp."

35 Amnesty International, "Encryption."

36 Ibid., 12; France, Law No. 2001-1062 (requiring, in French Criminal Code, disclosure of encryption keys on authorization by a judge); Spain, Law on Telecommunications 25/2007 (key disclosure); Turkey, Law No. 5651 on Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting (requiring encryption suppliers to provide copies of encryption keys to government regulators before selling encryption tools to users).

37 Dante D'Orazio, "China Passes Controversial Anti-Terrorism Law to Access Encrypted User Accounts," *The Verge,* December 27, 2015, http://www.theverge.com/2015/12/27/10670346/china-passes-law-to-access-encrypted-communications.

38 Emily Rauhala, "China Passes Sweeping Anti-Terrorism Law With Tighter Grip on Data Flow," *Washington Post,* December 28, 2015, https://www.washingtonpost.com/world/china-passes-sweeping-anti-terrorism-law-with-tighter-grip-on-data-flow/2015/12/28/4ac6fe06-d79b-4c4c-bda9-27f15fabf892_story.html?tid=a_inl.

39 Daniel Severson, "Encryption Legislation Advances in France," *Lawfare* (blog), April 14, 2016, https://www.lawfareblog.com/encryption-legislation-advances-france. ("Article 434-15-2 currently imposes a three-year prison term and a 45,000-euro fine for 'anyone who has knowledge of a secret decryption key for an encryption standard that may have been used to prepare, facilitate or commit a crime or offense' and who refuses to provide

or use such decryption keys in cooperation with the authorities. If cooperation would have prevented a crime or limited its effects, the penalties increase to five years in prison and a 75,000-euro fine.") See also Chertoff Group, "The Ground Truth About Encryption," 14 (discussing other states' demands for back-door keys).

40 Daniel Severson, "The World's Not Waiting for California: France Moves to Enforce Decryption," *Lawfare* (blog), March 7, 2016, https://www.lawfareblog.com/worlds-not-waiting-california-france-moves-enforce-decryption.

41 Draft Investigatory Powers Bill, November 2015, clause 189. See also clause 190 (requiring secretary of state to take into account "the technical feasibility of complying with the notice").

42 Ibid., clause 189(4)(c).

43 "Fact Sheet: Investigatory Powers Bill: Obligations on Communications Service Providers (CSPs)," https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/530557/Obligations_on_CSPs_Factsheet.pdf.

44 Matt Burgess, "Home Office Will Make 'Major' Changes to Revised Surveillance Bill," *Wired,* March 1, 2016, http://www.wired.co.uk/article/home-office-investigatory-powers-bill.

45 See, e.g., FBI Director James Comey, "Expectations of Privacy: Balancing Liberty, Security, and Public Safety," speech at Kenyon College, Gambier, Ohio, April 6, 2016, https://www.fbi.gov/news/speeches/expectations-of-privacy-balancing-liberty-security-and-public-safety. ("I love strong encryption. It protects us in so many ways from bad people.")

46 Susan Hennessey, "Draft Feinstein-Burr Encryption Bill Is Here," *Lawfare* (blog), April 8, 2016, https://www.lawfareblog.com/draft-feinstein-burr-encryption-bill-here; for the bill itself, see: https://lawfare.s3-us-west-2.amazonaws.com/staging/2016/Burr%20Feinstein%20Draft%201.pdf.

47 For criticisms, see, e.g., Paul Rosenzweig, "The Incredible Breadth of Feinstein-Burr," *Lawfare* (blog), April 12, 2016, https://www.lawfareblog.com/incredible-breadth-feinstein-burr; Julian Sanchez, "Feinstein-Burr, Encryption, and 'The Rule of Law,'" *Just Security* (blog), April 19, 2016, https://www.justsecurity.org/30669/feinstein-burr-encryption-the-rule-law/. But see 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.

48 See Comey, joint statement, "Going Dark" ("In limited circumstances, this investment [in developing tools and techniques to address end-to-end encryption] may help mitigate the risks posed in high priority national security or criminal cases, although it will most likely be unable to provide a timely or scalable solution in terms of addressing the full spectrum of public safety needs."); Groll, "WhatsApp" ("Clandestine methods used by intelligence agencies cannot be used in court as evidence, and the FBI has far more stringent restrictions on how it operates on U.S. soil").

49 One exception is the Joint Statement by EUROPOL and the European Union Agency for Network and Information Security, May 20, 2016, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection. That document takes a measured approach to the competing equities of law enforcement and data security and privacy.

50 Jennifer Daskal and Andrew Woods, "A New US-UK Data Sharing Treaty?" *Just Security* (blog), June 23, 2015, https://www.justsecurity.org/24145/u-s-u-k-data-sharing-treaty/.

51 Chertoff Group, "Ground Truth About Encryption," 11 ("[A] U.S.-ordered encryption access system would not be globally pervasive."); ibid., 13 ("If the U.S. government demands extraordinary access, even by placing the keys in escrow, how do we argue against other nations going to U.S. companies for the same access for what they believe and would describe as legitimate law-enforcement efforts?").

52 See, e.g., House Homeland Security Committee, "Going Dark Going Forward," 12; Chertoff Group, "Ground Truth About Encryption," 11. ("Perhaps more importantly, a U.S.-ordered encryption access system would not

be globally pervasive. Malicious actors would have other options for encrypted communication applications if they chose. . . . For these reasons, we think that requiring exceptional access is unlikely to be as productive as law enforcement hopes it will be—at least when it comes to determined and motivated actors.")

53 Sean Lyngaas, "NSA's Information Assurance Directorate at a Crossroads," *FCW,* January 26, 2016, https://fcw.com/Articles/2016/01/26/nsa-iad-lyngaas.aspx?Page=1 (describing role of NSA in helping to secure critical infrastructure and advise private sector about discovered vulnerabilities); UK Government Communications Headquarters (GCHQ) Director Robert Hannigan, "Front Doors and Strong Locks: Encryption, Privacy and Intelligence Gathering in the Digital Era," speech at MIT, March 7, 2016, https://www.gchq.gov.uk/speech/front-doors-and-strong-locks-encryption-privacy-and-intelligence-gathering-digital-era. ("From traditional protection of military communications, through personal privacy online—including identity verification for those critical Government digital services—through the security of domestic 'smart' power meters and electricity meters—where the design principle is that homeowners are in control of their data—to the security of the nuclear firing chain at the high end, we understand the importance of encryption for the economy and for the individual. That importance grows as more of our private lives move online and the economy becomes increasingly dependent on digital currency and block-chain systems. We advise government, industry, and individuals on how to protect their information appropriately.")

54 Hannigan, "Front Doors and Strong Locks."

55 Charles Arthur, "China Tightens 'Great Firewall' Internet Control with New Technology," *The Guardian* (UK), December 14, 2012, https://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control; "China Blocks Virtual Private Network Use," *BBC News,* January 26, 2015, http://www.bbc.com/news/technology-30982198 (stating that China blocks virtual private networks [VPNs], which rely on dedicated encryption links between users); Ellen Messmer, "Encryption Restrictions," *Network World,* March 15, 2004, http://www.networkworld.com/article/2331257/lan-wan/encryption-restrictions.html (describing corporations that have been dissuaded from using encryption in China and citing Chinese officials as stating that encryption restrictions are aimed at Chinese citizens).

56 Josh Horwitz, "WhatsApp's Encryption Could Make It a Target of the Chinese Government," *Quartz,* April 6, 2016, http://qz.com/655778/whatsapps-encryption-could-make-it-a-target-of-the-chinese-government/ (reporting that China detained human rights lawyers who used Telegram, an encryption-enabled application).

57 Sara Zaske, "While US and UK Governments Oppose Encryption, Germany Promotes It. Why?" *ZDNet,* October 26, 2015, http://www.zdnet.com/article/while-us-and-uk-govts-oppose-encryption-germany-promotes-it-why/ ("There's an official sanction on the part of the German authorities for encryption that keeps you out of sight of Anglo-Saxon eyes."); *Der Spiegel* staff, "Prying Eyes: Inside the NSA's War on Internet Security," *Der Spiegel,* December 28, 2014, http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html (quoting Michael Hange, president of the Federal Office for Information Security, as stating, "We suggest cryptography—that is, consistent encryption"). For the Netherlands, see House Homeland Security Committee, "Going Dark Going Forward," 14.

58 Alina Selyukh and Steve Henn, "After Paris Attacks, Encrypted Communication is Back in Spotlight," NPR, November 16, 2015, http://www.npr.org/sections/alltechconsidered/2015/11/16/456219061/after-paris-attacks-encrypted-communication-is-back-in-spotlight.

59 James Eng, "NSA Chief Mike Rogers: Encryption Is 'Foundational to the Future,'" *NBC News,* January 21, 2016, http://www.nbcnews.com/tech/security/nsa-chief-mike-rogers-encryption-foundational-future-n501391.

60 Jose Pagliery, "Ex-NSA Boss Says FBI Director Is Wrong on Encryption," *CNNMoney,* January 13, 2016, http://money.cnn.com/2016/01/13/technology/nsa-michael-hayden-encryption/.

61 Mike McConnell, Michael Chertoff, and William Lynn, "Why the Fear Over Ubiquitous Data Encryption Is Overblown," July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html. See also "Liberty and Security in a Changing

World," President's Review Group on Intelligence and Communications Technologies, December 12, 2013: 22, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf ("The US Government should take additional steps to promote security, by (1) fully supporting and not undermining efforts to create encryption standards; (2) making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption; and (3) supporting efforts to encourage greater use of encryption technology for data in transit, at rest, in the cloud, and in storage").

62 Sara Sorcher and Joshua Eaton, "What the US Government Really Thinks About Encryption," *Christian Science Monitor,* May 25, 2016, http://m.csmonitor.com/World/Passcode/2016/0525/What-the-US-government-really-thinks-about-encryption.

63 Jose Pagliery, "NSA is world's best hacker thief, says former director," *CNNMoney,* January 12, 2016, http://money.cnn.com/2016/01/12/technology/nsa-michael-hayden-us-hacker-thief/; Dan Goodin, "How the NSA Can Break Trillions of Encrypted Web and VPN Connections," *Ars Technica,* October 15, 2015, http://arstechnica.com/security/2015/10/how-the-nsa-can-break-trillions-of-encrypted-web-and-vpn-connections/.

64 McConnell, Chertoff, and Lynn, "Fear is Overblown."

65 Russell Brandom, "Why the NSA Is Staying Out of Apple's Fight with the FBI," *The Verge,* March 9, 2016, http://www.theverge.com/2016/3/9/11186868/apple-fbi-nsa-encryption-exploit-hack.

66 To be fair, the NSA faces certain legal and policy constraints that some foreign intelligence agencies do not. US officials must respect the First Amendment; states such as the United Kingdom have no similar limitation. China has erected the Great Wall and enjoys the intelligence collection advantages of a totalitarian government.

67 Chertoff Group, "The Ground Truth About Encryption," 11. See also ibid., 18.

68 For a discussion of the factors that have led states to decline to develop international rules related to intelligence, see Ashley Deeks, "An International Legal Framework for Surveillance," *Virginia Journal of International Law* 55, no. 2 (2015): 291.

69 Loch K. Johnson, "Think Again: Spies," *Foreign Policy,* November 9, 2009: 18.

70 See Letter from UN Special Rapporteurs to Russian Ambassador Alexey Borodavkin, July 28, 2016, http://www.ohchr.org/Documents/Issues/Opinion/Legislation/RUS_7_2016.pdf (describing recently enacted "Yarovaya Law," which requires Internet service providers to maintain capacity to provide Russian security service with keys to all encrypted messages sent by users); "Russian Laws and Regulations: Implications for Kaspersky Labs," *Wired,* 2012, http://www.wired.com/images_blogs/dangerroom/2012/07/Russian-Laws-and-Regulations-and-Implications-for-Kaspersky-Labs.pdf ("Individuals and legal entities in Russia, providing postal services, telecommunications of all kinds, including systems, data communication, confidential, satellite communications, are obliged at the request of the Federal Security Service to include in the extra hardware equipment and software, as well as create other conditions necessary for the operational and technical measures by the Federal Security Service"; emphasis omitted).

71 See, e.g., Michelle Wein and Stephen Ezell, "How to Craft an Innovation Maximizing T-TIP Agreement," Information Technology & Innovation Foundation, October 2013, http://www2.itif.org/2013-innovation-maximizing-ttip-agreement.pdf (arguing for trade treaty provisions that prevent restrictions on the import or use of commercial encryption technologies and encouraging a "flexible, global approach in those narrow circumstances where regulation may be justified (e.g., certain government or military uses)").

72 Ibid., 6 (noting that one reason to support free trade is the belief that reducing tariffs and non-tariff barriers promotes innovation because it lowers the costs of products overseas and thus allows innovators access to a broader market).

73 Some European companies, such as Deutsche Telekom, appear to share this view. "Encryption for the People: Telekom and Fraunhofer unveil 'Volksverschulüsselung,'" *Deutsche Welle,* June 29, 2016, http://www.dw.com

/en/encryption-for-the-people-telekom-and-fraunhofer-unveil-volksverschlüsselung/a-19363984 (describing Deutsche Telekom's encryption project).

74 Richard Cowan, "U.S. Tech Industry Appeals to Obama to Keep Hands Off Encryption," Reuters, June 9, 2015, http://www.reuters.com/article/us-cybersecurity-usa-encryption-idUSKBN0OP09R20150609.

75 Ibid.

76 Ibid.

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

78 In the Matter of the Search of an Apple iPhone, E.D. No. CM 16-10 (SP), Government's Motion to Compel Apple to Comply 2–3, https://www.wired.com/wp-content/uploads/2016/03/2016.03.10-149-Gov-Reply-ISO-Mot-to-Compel-Opp-to-Apple-Mot-to-Vacate.pdf; also see Alina Selyukh, "DOJ Lays Out Its Legal Case For Why Apple Should Help Crack An iPhone," NPR, February 19, 2016, http://www.npr.org/sections/thetwo-way/2016/02/19/467385553/doj-lays-out-its-legal-case-for-why-apple-should-help-crack-an-iphone.

79 See Amul Kalia, "Where Do Major Tech Companies Stand on Encryption?" Electronic Frontier Foundation, October 9, 2015, https://www.eff.org/deeplinks/2015/10/where-do-major-tech-companies-stand-encryption (listing positions of twenty-one major technology companies on end-to-end encryption).

80 Comey, joint statement, "Going Dark."

81 NSC Draft Options Paper, *Washington Post.*

82 This appears to be the first free trade agreement that specifically addresses encryption.

83 Trans-Pacific Partnership Agreement, Annex 8-B.

84 Ibid., Annex 8-B, section A.3.

85 Ibid., Annex 8-B, section A.5.

86 Ibid., article 29.2(b).

87 See, e.g., Stewart Baker, "USTR Wins the Crypto War," *Washington Post,* November 6, 2015, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/11/06/ustr-wins-the-crypto-war/?utm_term=.3946124ee728 (suggesting that states-parties to TTP may not demand back-door access); Jeremy Malcolm, "Has the TPP Ended the Crypto Wars? Hardly," Electronic Frontier Foundation, November 18, 2015, https://www.eff.org/deeplinks/2015/11/has-tpp-ended-crypto-wars (suggesting that states-parties may do so); Simon Lester, "The TPP and Encryption," *Cato at Liberty* (blog), Cato Institute, November 18, 2015, http://www.cato.org/blog/tpp-encryption (arguing that language is ambiguous and its meaning will be worked out in litigation).

88 The Wassenaar Arrangement, Participating States, http://www.wassenaar.org/participating-states/ (last visited September 27, 2016).

89 Sarah Andrews, "Who Holds the Key? A Comparative Study of US and European Encryption Policies," *Journal of Information, Law and Technology,* February 29, 2000, http://encryption_policies.tripod.com/international/andrews_290200_key.htm.

90 The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Dual-Use List, Category 5, Part 2, "Information Security," Note 4, http://www.wassenaar.org/wp-content/uploads/2016/07/WA-LIST-15-1-CORR-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf.

91 Encrypted hardware is on the Export Administration Regulations Commerce Control List at 5A002; encrypted software is at 5D002. "Understanding Export Controls for Encryption," http://www.export.gov/webinars/eg_main_046622.asp (updated November 21, 2012).

92 Lin, “Brennan’s Recent Testimony on Encryption.”

93 Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar, “A Worldwide Survey of Encryption Products,” February 11, 2016, https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf (also concluding that “both domestic and foreign encryption products regularly use strong published encryption algorithms such as AES”).

94 Ibid.

95 Harold Abelson et al., “Keys Under Doormats,” 3. (“A vibrant legal system with respect for the rule of law is necessary for privacy protection in the face of ever more powerful electronic surveillance technologies. Which countries have sufficient respect for the rule of law to participate in an international exceptional access framework?”)

The preferred citation for this publication is:
Ashley Deeks, "The International Legal Dynamics of Encryption," Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1609 (October 12th, 2016), available at https://lawfareblog.com/international-legal-dynamics-encryption.

About the Author

ASHLEY DEEKS

Ashley Deeks is an Associate Professor at the University of Virginia Law School. She previously served in the U.S. State Department as the assistant legal adviser for political-military affairs, among other positions. Deeks was a 2007–08 Council on Foreign Relations International Affairs Fellow. She serves on the State Department's Advisory Committee on International Law and is a senior contributor to the Lawfare blog.

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 group's output will also be published on the Lawfare blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

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