Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects

A HOOVER INSTITUTION ESSAY

Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects

RYAN BUDISH, HERBERT BURKERT, AND URS GASSER

Aegis Series Paper No. 1804

Introduction

In the wake of the 2016 San Bernardino shooting, Apple and the US Federal Bureau of Investigation waged a public battle over the availability of essentially unbreakable encryption in consumer devices.[1] Ultimately the FBI was able to access the contents of the phone.[2] This forestalled proposed changes to US law and policy that would have effectively changed the level of encryption available in American consumer technologies.[3] Throughout this tense domestic debate—involving a US crime, US law enforcement, a US company, and US law—there was only a vague sense of what the broader international implications might be.[4] As the Trump administration considers reopening the debate over US encryption policies, and as many countries around the world consider and implement their own encryption policies, it is more important than ever to understand the ways in which seemingly domestic encryption policy decisions can reverberate around the globe.[5]

The recent scuffles over iPhone encryption are just one set of examples of the ways in which new consumer technologies with built-in encryption have created novel challenges for law enforcement agencies, national security agencies, and other policy-makers. In response to these technological challenges, policy-makers are increasingly considering policies with direct and indirect impacts on the effectiveness of encryption tools. While the domestic impacts of such policies are often intended and predictable, the international implications are often both unintentional and poorly understood. In an interconnected, highly networked world, it is no surprise that domestically focused policies can have significant international implications, but there is much that we do not yet understand about those international implications. This knowledge gap limits sound, evidence-based policy-making. Decision-makers often push encryption policies without a clear appreciation for the numerous global ramifications, including ripple effects that can undermine the original intent of the policy.

We would like to thank Amy Zhang, Jacqueline Abreu, Katie Blenko, Stanislav Budnitskiy, Michelle Forelle, and Michelle Ng for their excellent research assistance.

By way of select examples, this paper explores the potential international ripple effects of domestic policy changes. In some cases, these changes take the form of a single coherent national policy, while in other cases they are a collection of multiple independent (or even conflicting) policies. In either case, as countries consider encryption policies, it is important to develop a more concrete approach for understanding their range of impacts. To that end, this paper offers a conceptual model for how those ripple effects might propagate beyond national borders. First, we offer a brief background on encryption policies. Next, we explore the potential ripple effects using a three-step approach: (1) we look at the variety of instruments through which a country can implement encryption policy (including, but not limited to, law and regulation); (2) we examine the variety of pathways and relationships through which encryption policy can have international effects; and (3) we consider a series of examples from around the world that illuminate some of the complexities and variations of these ripple effects. From these examples, it becomes clear that a single encryption policy can involve a variety of regulatory instruments, relationships, and pathways, plus numerous cascading ripple effects. In order to help policy-makers think about these effects in a useful and actionable way, in a subsequent section we apply our framework to develop a set of factors that can help policy-makers anticipate some of the most likely ripple effects of proposed encryption policies. The last part summarizes and concludes.

A Brief Background on Encryption Policies

Discussing the potential effects of encryption policies requires that we first address two related and foundational questions: What are the policy objectives driving those policies? And what do we mean by "encryption policy?" This paper adopts a broad definition of encryption policy because a narrower definition would exclude many formal and intentional actions that a government might take to advance its policy objectives even if those actions might not take the form of law or regulation. Although such an inclusive approach complicates the analysis, it reflects the important reality that a government can advance its policy objectives though a range of direct and indirect activities, and the ripple effects of those activities, can be significant.

Encryption policies can be either directly or indirectly advanced in relation to a wide range of policy objectives. Although examples like the Apple-FBI dispute over the availability of unbreakable encryption in consumer products highlighted the national security elements of the debate, encryption policies can be motivated by concerns over law enforcement's inability to fully investigate criminal activity, efforts to advance economic competitiveness, desires to advance and support technological innovation, responses to geopolitical developments such as the disclosures from Edward Snowden, objections to the current mechanisms and institutions of Internet governance, and worries about the future interoperability of the Internet. Whether certain policy objectives are normatively desirable and whether the proposed policies successfully advance those objectives are questions that are inherently tied to geopolitical, economic, and social contexts, and are thus beyond the

scope of this paper. This paper is concerned solely with the international ripple effects from encryption policies, not the merits of the policies themselves.

Capturing the ways in which these myriad policy objectives can indirectly—and yet significantly—shape the use of encryption requires that we adopt a broad definition of encryption policy. Consider the PRISM and Upstream programs, two types of government surveillance revealed by Edward Snowden as authorized activities under Section 702 of the FISA (Foreign Intelligence Surveillance Act) Amendments Act. A narrow definition of encryption policy might exclude Section 702, given that it was not directly written to encompass encryption, nor were its impacts on encryption embodied in explicit law or regulation. Instead, the policy objectives behind Section 702 were explicitly about national security. Advancing those policy objectives necessitated a series of knowing and intentional choices about encryption that had a significant impact, both domestically and internationally, on data in transit and data at rest. A narrower definition of encryption policy would miss the range of institutional activities—like those covered under Section 702—that can indirectly yet intentionally affect the use of encryption. For that reason, this paper includes within the scope of encryption policy the full array of government activities that either support or hinder the development, use, and adoption of encryption technologies, and that collectively reflect a normative judgment on the part of government about the value of such technologies.[6]

Before exploring the ripple effects of encryption policies, it is important to note the broader and increasingly international encryption technology environment. A recent publication of the Berkman Klein Center for Internet & Society surveyed 865 hardware and software encryption products around the world.[7] Of those 865 products, 546 products were from fifty-four countries other than the United States. Notably, the encryption architecture did not vary substantially from country to country, meaning that comparable levels of protection were available from different products in different countries. Additionally, many of the companies whose products were surveyed are "jurisdictionally agile" and are able to relocate their operations quickly and easily. We take special note of this diversity and agility, as this low-friction environment enables many of the ripple effects we describe below.

Encryption Policy Ripple Effects

Although encryption policy can have an array of international ripple effects, those effects often begin with an action that is primarily domestically and internally oriented.[8] For example, a law enforcement agency seeking the tools necessary to investigate domestic criminal activity or an intelligence agency seeking assistance from domestic companies both reflect domestic-oriented policies. Even an encryption policy such as an export ban, which has an obvious extraterritorial impact on would-be importers, constrains *domestic* company behavior to preserve a *domestic* technological advantage. These domestic-centric policies, however, create effects that spill beyond national borders. In some cases, these

ripple effects may be intentional, but in many others they are unintentional and even unexpected.

In order to better articulate and understand these ripple effects, in this part we offer a rudimentary framework for conceptualizing encryption policies. We begin by identifying the basic instruments of encryption policy. Next, we look at the pathways and relationships through which the economic, political, and technological effects of those tools can ultimately affect another country's policies. Finally, we apply this framework to a series of country-specific examples to show some of the diversity of these ripple effects.

Instruments of Encryption Policy

As described below, we adopt an expansive definition of encryption policy that includes more than just the laws and formal regulations that specifically target encryption. Instead, encryption policy encompasses the use of a variety of regulatory instruments. These instruments can be, and indeed often are, deployed in parallel in a variety of configurations. Moreover, given that governments may have a variety of agencies, each pursuing its own encryption policy, these instruments are not always deployed in a consistent manner within a single jurisdiction. Below, we identify a few of these instruments that policy-makers use to try to shape encryption policy.

Law and formal regulation: This regulatory instrument involves the variety of ways that governments can either enact or enforce laws and regulations in order to strategically constrain or direct the development and use of encryption technologies. This regulatory instrument directly applies only to those entities under the jurisdiction of the regulator or lawmaker. Examples of this include legislative proposals in the United States in the mid-1990s that would have required new digital technologies to be capable of being wiretapped and the FBI's attempt to use the All Writs Act to obtain a court order to compel Apple to decrypt the San Bernardino shooter's iPhone in 2016.[9]

Procurement power: This regulatory instrument involves the use of a government's sometimes substantial spending power to influence local and global markets and encourage companies to change their products to meet government procurement regulations. For example, the National Security Agency (NSA) in the United States designates certain kinds of encryption technologies as suitable for certain government uses.[10]

Hegemonic status: This regulatory instrument involves the exercise of political, economic, and military strength to project encryption policies beyond national borders. It can be an effective instrument when the policy objectives require compelling the behavior of actors who might not be affected by legislation and regulation (or could easily escape its jurisdiction). An example of the use of hegemonic status is Russia's success in convincing its geographic neighbors to adopt policies similar to its own.

Soft power: This regulatory instrument involves convincing actors to comply with encryption policies through persuasion and other voluntary means. It is particularly effective after significant geopolitical events that leave actors open to persuasion that such policies are necessary for the greater good. For example, several American companies may have voluntarily provided some data to the US government in the years following the terrorist attacks of September 11, 2001.[11] In addition to national security arguments, companies have generally shown a willingness to cooperate with government agencies for compelling reasons such as facilitating child pornography investigations or missing person cases.[12] The perception of policies and power dynamics can have amplifying or mitigating effects on the potency of soft power as an instrument of encryption policy.

Multilateral treaties: This regulatory instrument involves countries working together to collaboratively draft and adopt agreements that effectuate a standardized policy between signatories. For example, the Wassenaar Arrangement is a multinational agreement which limits the export of certain kinds of technologies, including certain kinds of encryption.[13]

Standard-setting and multi-stakeholder organizations: This regulatory instrument involves governments collaboratively advancing encryption policies with the input, feedback, and buy-in of a variety of stakeholders, including the private sector, civil society, academia, and others. For example, the US National Institute for Standards and Technology (NIST) "works closely with experts in industry, academia and government to develop its cryptographic standards and guidelines."[14]

Pathways of Ripple Effects

One reason why the international ripple effects of encryption policy can be so complex is that the regulatory instruments described above can implicate and affect a variety of actors and relationships across the world. Understanding the potential ripple effects from encryption policies requires a greater understanding of the pathways and relationships that each of these regulatory instruments might activate and through which ripple effects propagate outward across boundaries. Rather than attempting to exhaustively list these—an impossible feat, given the numerous dependencies between international commerce, geopolitical power dynamics, and technical developments that help account for the ripple effects of encryption policy—we identify seven such pathways and relationships to start.

1. National encryption policy directly affects another country's public policy.

2. National encryption policy directly affects another country's private sector.

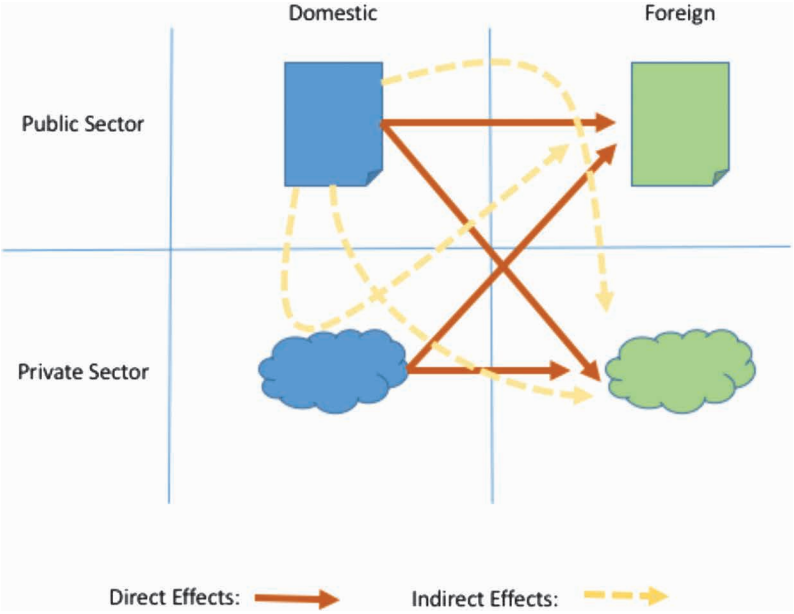
3. National encryption policy indirectly affects another country's public policy through an impact on the domestic private sector.

4. National encryption policy indirectly affects another country's private sector through an impact on the domestic private sector.

5. National encryption policy indirectly affects another country's private sector through an impact on that country's public policy.

6. Private sector policies directly affect another country's private sector.

7. Private sector policies directly affect another country's public policy.



Source: Ryan Budish

Examples: Ripple Effects of Encryption Policy

The policy instruments and pathways we have identified interact to create the complex ripple effects of encryption policies. In order to illustrate how the various elements described above come together to create the ripple effects of encryption policy, we highlight below a few examples from selected regions around the world.

We recognize that the ripple effects of some countries may be stronger, and therefore more identifiable, than others. In the examples below, we observe an outsize influence from the United States and China, likely due to their hegemonic power over global markets and international privacy and national security norms, which engender spillover effects from domestic encryption policy that more acutely affect other countries. In contrast, the effects of encryption policies propagating from other countries are sometimes less clear.

Below, we look at the ways various countries deploy the instruments of encryption policy through the pathways identified to craft policies with domestic intent that create (1) economic, (2) political, and (3) technological effects that extend well beyond national borders. We first address the perspective of the United States and document the major encryption policy events that have triggered ripple effects in other countries. From there, we switch perspectives and examine how the encryption policies of other countries have affected, albeit to a lesser degree, the private and public sectors beyond its borders. These examples were selected for their geographic diversity and ability to highlight different ways in which the ripple effects can propagate, but they remain only illustrative.

America's Encryption Policy and Its Ripple Effects

The United States does not have a single, consistent encryption policy. Instead, the government's approach to encryption has played out piecemeal across multiple government and corporate actors utilizing several different regulatory instruments. Some have had significant international impacts.

The most dramatic ripple effects propagating from the United States can be observed in the aftermath of Edward Snowden's revelations of the US government's surveillance efforts.[15] Consider once more the NSA's PRISM program authorized under Section 702 of the FISA Amendments Act, which provided the agency access to the content and user information of several US-based technology companies.[16] In setting up this program, the NSA is believed to have used both soft power to convince companies to assist in intelligence gathering—an argument that carried understandable weight immediately following the terrorist attacks of September 11, 2001—and legal force to compel companies that did not voluntarily participate.[17] When newspapers revealed the existence of the program, the fallout had political, technological, and economic dimensions. Domestically, the pervasive US government surveillance was attacked as an example of perceived US control over the Internet and was used as a rationale to support proposed reforms to both the structure and governance of core components of the Internet.[18] At the same time, analysts predicted the economic impact on US companies from the Snowden revelations to range from $35 billion to $180 billion in lost revenue.[19]

US encryption policy has also been shaped by the government's participation in standard-setting organizations that have helped direct the development of encryption tools. In one case, the NSA advocated for adoption of the Dual_EC_DRBG algorithm. When it was later discovered that this algorithm had significant weaknesses, some experts highlighted the possibility that the NSA advocated for the algorithm because it knew of the weaknesses and could exploit them.[20] Although the NSA's motivations cannot be determined, the accusations compounded existing trust deficits, potentially undermining all government contributions to such organizations.[21]

Specialized government expertise can also have an impact on encryption policy through influence over government procurement. For example, in 2015, the NSA stopped recommending that government agencies use certain encryption algorithms, asserting that they could be vulnerable to certain attacks by quantum computers.[22] While there are questions about how the NSA reached this conclusion, the recommendation affected both technologically and economically a variety of government agencies and the companies that provide services to them.

US encryption policy is also directly shaped by companies. One notable example, mentioned at the outset, was the fight between Apple and the FBI over access to the San Bernardino shooter's encrypted iPhone. Given the expected economic fallout from the Snowden revelations, it was perhaps unsurprising that companies like Apple would make technological changes to their products in order to reassure customers. Apple's decision to offer end-to-end encrypted messaging and full device encryption, both enabled by default, could be seen as a direct response to declining consumer trust and concerns over NSA surveillance.[23] In order to compel Apple to provide access to the San Bernardino shooter's iPhone data, the FBI tried to use several instruments: supporting legislative changes, requesting court orders, and engaging in a media offensive.[24] However, Apple remained steadfast in its refusal, and the FBI dropped the case after failing to win court approval and accessing the data through other means. This exchange highlights both the role that companies have in shaping encryption policy and the feedback loops that exist as domestic policy creates international ripple effects that can then influence domestic actors such as Apple.

The response of other countries to these events provides strong evidence of the international ripple effects of US encryption policy.

Political Effects In the European Union, newly proposed encryption policies have largely been defined as political reactions to the Snowden disclosures, the Apple-FBI debate, and recent terror attacks.[25] For example, as encryption moved to the forefront of global debates, various countries proposed unilateral measures that represented both staunch opposition to, and support of, encryption technology. The United Kingdom's Investigatory Powers Act, introduced in 2016, included a provision about the removal of "electronic protection applied by or on behalf of that operator to any communications or data," which could lead to fines for tech companies unwilling or unable to decrypt user data.[26] As part of France's Digital Republic Act, provisions that would have mandated encryption backdoors and data localization were only narrowly defeated.[27] Similarly, legislation in Hungary that would have limited the use of end-to-end encryption was only changed following strong objections.[28] In the Netherlands, the government argued that it is not "desirable to take legal measures against the development, availability and use of encryption."[29] In Germany, the government called for "more and better encryption" as revelations surfaced about the surveillance of Chancellor Angela Merkel's phone.[30]

Political ripple effects were also observed in China. After having previously backed off their demands for backdoors in encryption, the Chinese government closely watched the outcome of the Apple-FBI debate.[31] And in 2017, China's State Cryptography Administration released a draft encryption law that would enable certain departments of the government to "require telecommunications companies and Internet service providers to provide 'decryption technology support.'"[32]

Technological Effects The technological effects from US encryption policies are visible as well. For example, due to concerns over the potential vulnerabilities in the US-backed Dual_EC_DRBG encryption standard after the NSA revelations, the Brazilian government discreetly ceased use of certain NSA-endorsed encryption techniques.[33] In order to fill the gap, Brazil adopted the German cryptography standard Brainpool, sponsored by Germany's NIST-equivalent BSI.[34] The Brazilian Intelligence Agency also encouraged government officials to use two national cryptographic systems to secure government communications from foreign surveillance.[35] In both cases, the technological and economic ripple effects of US policies that weakened confidence in certain encryption technologies aided local Brazilian and German businesses at the expense of US companies.

Economic Effects As mentioned above, the economic impact of recent US encryption policy events on American companies is expected to be substantial—an estimated $35 billion to $180 billion in lost revenue for US companies. But there is also strong evidence of effects on the private sectors of other countries as well. These economic impacts have been apparent in the software and cloud services industries, where switching costs can be relatively low. A survey of one thousand IT decision-makers from the United Kingdom, France, Germany, Hong Kong, and the United States found that 97 percent of respondents in the European Union, 92 percent in the United States, and 69 percent in Hong Kong were changing their methods for managing data, and now preferred buying cloud services located in their own regions.[36] Similarly, a move away from US-developed technologies has created an opening for crypto-entrepreneurs marketing new encryption services. Several non-American encryption technology companies experienced significant increases in their user bases after the full extent of NSA spying was revealed.[37] And in India, planned partnerships between Google and Indian election officials to improve voter registration were abandoned.[38]

The economic effects have also extended to hardware. Cisco sales of routers dropped by 10 percent following the Snowden leaks.[39] And in Russia, the government has expressed its distrust of Intel and AMD processors following the revelations, replacing Intel systems with homegrown microprocessors and moving to Linux-based operating systems.[40] In Germany, the government ended a major contract with Verizon Communications in 2014 over concerns of network security. It replaced Verizon's business providing communications services to government agencies with the services of the German phone giant Deutsche Telekom AG, which is a Verizon rival.[41]

Ripple Effects from Encryption Policies of Other Countries

Although the United States serves as a strong source of ripple effects, we have selected a geographically diverse set of examples to highlight other ways countries utilize instruments and pathways to enact encryption policies that create international ripple effects.

The European Union As of December 2017, there are currently no European Union-wide rules on encryption. That said, the matter is far from settled and there are ongoing efforts to define that policy at both the national and EU-region levels. More important, we see from recent policy debates over privacy and cybersecurity that the European Union can have significant international ripple effects, as single-country decisions can quickly ripple across the region. Additionally, as the European Union builds a digital single market, its policies can create ripple effects well beyond the member states.

Following a string of terror attacks over the past few years, several countries began to pressure the European Commission for legal rules that would grant to law enforcement agencies greater access to encrypted online communications. Several of these attacks—including the November 2015 Paris attack and the March 2017 attack in London—are believed to have been planned using encrypted communication tools such as WhatsApp.[42] Each prompted calls for new legal authorities. In late 2015, the UK Parliament passed the Investigatory Powers Act (IPA), which does not ban encryption outright but leaves several open questions regarding the government's ability to compel company cooperation.[43] And more recently, the UK government has urged the European Union to act as well.[44] The interior ministers of France and Germany have echoed such calls, seeking the same rights to access online communications as are available from telecom companies for telephones.[45] Additionally, Poland, Hungary, Croatia, Latvia, and Italy have all urged the European Commission to propose new encryption legislation.[46] In response to these calls, the EU Justice Commissioner intended to propose three or four options by June 2017 that would address some of these issues.[47] As of that date, however, the "expert process on encryption" was expected to continue over several more months.[48]

In exercising this soft power, these countries are advancing new regional policies that would likely affect the use of encryption both within and outside the European Union. The extraterritorial impacts of EU privacy and cybersecurity policies demonstrate this potential. Following the adoption of the 1995 Data Protective Directive 95/46/EC, national governments in all member states to the European Union, as well as the additional member countries of the European Economic Area (Norway and Liechtenstein), have implemented compliant national laws.[49] On the cusp of the 2018 enforcement of the General Data Protection Regulation, which supplants the 1995 directive, we see more clearly the impact of these rules outside of the European Union. Countries such as Argentina, Nigeria, Japan, and South Korea have all adopted complementary privacy laws.[50] Any business that targets European consumers needs to comply with the EU regulations.[51]

In another example, the European Commission's 2013 Cybersecurity Strategy for the European Union demonstrates an attempt at using similar policy tools in order to reshape the global cybersecurity marketplace.[52] The strategy was the first comprehensive policy document meant to strengthen the information systems in the European Union, build confidence in online services, and foster collaboration among international partners, the private sector, and civil society. An important aspect of the plan was to stimulate the development and deployment of encryption technology to ICT products in the European Union. In particular, the strategy aims to leverage the procurement power of the region's Digital Single Market in order to bolster the European Union's cybersecurity market and influence the global market of security products.[53] Additionally, the strategy calls for the use of multi-stakeholder approaches in further developing cybersecurity strategies and standards throughout the region, further influencing private sector companies that operate within Europe.[54]

These examples from slightly different contexts highlight how the current debate over encryption may ripple across Europe and beyond. Nonmember states with close economic relationships with the European Union, such as Norway and Switzerland, and candidate states such as Turkey and Ukraine have strong incentives to adopt EU policies. And economically, the European Union represents the world's largest single market with the potential to influence the supply and demand of encryption products.

India India's government has yet to establish a comprehensive national encryption policy. The country does have a legal framework that governs electronic communications, but the legislation fails to outline specific encryption standards.[55] Instead, various governmental entities have implemented encryption regulations that are contradictory and rarely enforced. This fragmented approach has had economic, political, and technical ripple effects.

One example is the effort to use law and regulation to change Indian encryption policy.[56] In September 2015, the Department of Electronics and Information Technology (DeitY) proposed a national encryption policy draft that would have required that data be stored in plain text for ninety days prior to encryption. The draft was withdrawn only days after its release due to public outrage and privacy concerns.[57] Had this bill advanced, the ripple effects would have been both economic and technological, as the preliminary draft applied to all service providers that operate in India, regardless of domicile.[58] An updated draft of the policy has been rumored to exist but has yet to be publicly discussed.

India's use of hegemonic power to influence foreign entities is exemplified in the government's efforts to gain access to data stored on BlackBerry products. The Indian government called on Canada-based Research in Motion (RIM), the maker of BlackBerry products, to provide encryption keys that would grant the government access to consumer messaging services, including BlackBerry Messenger and BlackBerry Internet Service email.[59]

RIM initially resisted, and the conflict escalated until India's Ministry of Home Affairs and the Department of Telecommunications threatened to shut down BlackBerry sales and service in India in 2010. RIM conceded and within three years had set up local data centers, giving the Indian government access to browsing data, emails and attachments, and other information (although no access to BlackBerry's Enterprise Servers).

This conflict between RIM and the Indian government highlights the complex ways that encryption policy interacts with geopolitical and economic forces. At first, RIM was able to resist India's demands and the ripple effects of the policy were minimal. However, BlackBerry's global sales began to plummet as consumers in the United States and Europe shifted to Apple and Google products. India was one of the few markets where BlackBerry sales continued to grow in the late 2000s, weakening RIM's ability to resist Indian demands. Ironically, however, by the time the encryption agreement was finalized between the Indian government and RIM in 2013, BlackBerry products had dropped from 12.3 percent of India's market share to only 1.2 percent.[60] Success with RIM has also emboldened India to use its procurement and regulatory powers to persuade Skype, Google, Yahoo, and GitHub to change their encryption and privacy standards, although with limited success to date.[61]

Finally, there have been attempts to use the Indian court system to shape encryption policy. In response to WhatsApp's use of 256-bit end-to-end encryption in its messaging app, Sudhir Yadav, a right-to-information activist concerned with national security, filed a public interest lawsuit against WhatsApp.[62] The suit claimed that WhatsApp's 256-bit encryption violated the Department of Communications requirement that no individual or organization may use anything stronger than a 40-bit encryption key unless the government grants special permission and the decryption keys are disclosed.[63] Additionally, other Indian laws require that the government have the ability to intercept all messages in the interest of public safety. The use of end-to-end encryption would make it impossible for WhatsApp to comply.[64] On June 29, 2016, India's Supreme Court dismissed Yadav's case but urged him to file a complaint with the Telecom Disputes Settlement and Appellate Tribunal.[65] This patchwork of broad and potentially applicable laws creates a substantial risk that a court could choose to apply them to online services like WhatsApp, with significant economic and technical ripple effects. Within India, over seventy million people use WhatsApp monthly and 90 percent of smartphone users have downloaded the app.[66] If an Indian court were to mandate backdoor access, WhatsApp and its owner, Facebook, would be under enormous economic pressure to comply. If they did not comply and WhatsApp was banned, there would be a high likelihood of users shifting to other messaging applications, just as Brazilian users did when WhatsApp was temporarily banned in Brazil.[67]

Russia Russia's encryption policy has been developed as part of the country's broader information security framework, which over the last fifteen years has increasingly included restrictive laws pertaining to digital communication and the use of encryption. The motivations for these restrictions have included combating social and political vices,

such as child pornography, suicide, drug use, extremism, and terrorism.[68] The most recent developments have directly targeted the use of encryption by non-Russian companies operating within Russia.

In 2014, Russian President Vladimir Putin approved a data localization law. In 2016, he approved stringent "antiterrorist" legislation that covers a wide range of offline and online activities.[69] Notably, the latter law requires all companies in the business of transmitting encoded messaging—which technically encompasses any and all digital communications—to assist the Federal Security Service (FSS) with decrypting such communications. The application of these laws has already led to a ban on LinkedIn, a demand that the messaging application Telegram "hand over keys allowing the government to decrypt any communications transmitted over it," and demands that Facebook and Twitter localize data by 2018.[70] The direct application of these laws on non-Russian companies is already having substantial effects, with Twitter agreeing to comply and Facebook still deciding. Moreover, there are further economic ripple effects because much of the technology needed for the data localization requirements is currently unavailable in Russia, which presents a commercial opportunity for non-Russian companies.

The political ripple effects of the law are also significant, as they could ultimately lead to fragmentation of the Internet. Russia exercises significant hegemonic power within its region, and it has traditionally influenced the communication policies of its geographic neighbors through a variety of means, including multilateral forums, such as the Commonwealth of Independent States and the Shanghai Cooperation Organization. One result of this hegemonic influence is that Russian telecom companies are the dominant provider in many of Russia's neighboring countries. Thus, there is a risk that countries like Belarus, Kazakhstan, Kyrgyzstan, Ukraine, and Uzbekistan will adopt similar encryption policies, given that they have previously adopted Russian surveillance technologies and regulations.[71] And even if those countries do not explicitly adopt Russian encryption policies, individual telecom companies may comply. Over time, this may lead a bloc of nations to adopt technologies and policies that are increasingly incompatible with developments elsewhere. For example, global financial services rely on strong encryption technologies. Any weakening of those technologies may make it difficult for those entities to operate effectively in both Russia and its neighboring countries.

Brazil Brazil has used the court system to implement its encryption policy, particularly in response to WhatsApp's use of end-to-end encryption. On two recent occasions, Brazilian courts issued blocking orders forcing telephone operators in Brazil to block the popular messaging service due to the US company's failure to comply with wiretap orders.[72] The ripple effects of this policy were somewhat blunted by WhatsApp's current popularity in Brazil. Because 90 percent of smartphone owners use the app, the court orders were quickly reversed for the "disproportionality" of their punishment, which affected "millions of users." However, the ripple effects have also included negative economic and technical

impacts, as the bans boosted use of competitor Telegram's products. Some reports claim Telegram gained seven million new users during the court-ordered blocks on Whatsapp.[73]

China In recent years, the Chinese government has enacted a variety of cybersecurity and encryption measures. The size of China's market magnifies the ripple effects of its policy decisions, creating significant challenges for non-Chinese companies and other countries.

The Chinese government has often used law and regulation to deploy its encryption policy. For example, in July 2015, China announced a sweeping new National Security Law that called for a review of the domestic tech industry to ensure that all key network infrastructure and information systems were "secure and controllable." According to some experts, the law was a protectionist policy that granted Chinese authorities the power to demand source code from foreign companies.[74] A few months later, China passed its first comprehensive antiterrorism legislation, which required telecom and Internet companies to provide decryption support to state security agencies investigating terrorist activities.[75] In justifying the legislation, officials with the Legislative Affairs Commission of the National People's Congress pointed out similarities with several internationally recognized practices.[76] On November 7, 2016, China approved a stringent cybersecurity law that would allow the government to submit companies in a broad range of sectors to security reviews of equipment and data. It will require Internet operators to provide "technical support" to security agencies involved in criminal and national security investigations.[77] Foreign companies operating in China have raised concerns over this vague language, convinced the new law might mandate the installation of backdoors within their products. The law came into effect on June 1, 2017. Additionally, an April 2017 proposed encryption law would, if enacted, authorize government entities to "require telecommunications companies and Internet service providers to provide 'decryption technology support.'"[78]

These stringent policies are likely to affect foreign companies in the Chinese market as well as encryption policy abroad. On the one hand, non-Chinese companies face enormous pressure to abide by the restrictions. The country's large population, burgeoning economy, and considerable purchasing power allow it to project its hegemonic status. China represents 43 percent of the worldwide tech sector.[79] Multinational technology companies like Microsoft, Cisco, and IBM are unwilling to ignore this market power. Economically, experts say companies will be required to decide between exposing their data to governmental surveillance and leaving the market completely. Already, large US companies like Apple have agreed to certain reviews by China's Internet control bureau, which could set a precedent for other countries to do the same.[80]

On the other hand, companies under pressure from China may themselves wield political power in order to ultimately shape more favorable encryption policies. For example, some experts anticipate mounting pressure from US-based multinational companies on the US government to respond and defend against China's restrictive laws.[81] Perhaps acting

to preempt such backlash, in August 2016 a committee under the country's powerful cyberspace administration announced a decision to allow foreign corporations, including Microsoft, Intel, IBM, and Cisco, to participate in the drafting of cybersecurity rules related to encryption and big data, among other issues. That said, the influence of these companies within the committee remains to be seen.[82]

China has also used its significant procurement power to influence global encryption policy. The country announced a five-year plan to wean the country off foreign technology and replace foreign firms with domestic ones by 2020.[83] In response to news reports alleging that American and British intelligence agencies had hacked into a private company and obtained the encryption keys to millions of SIM cards used in mobile devices around the world, China immediately began investing in domestic alternatives. Similarly, in 2015 China dropped major US tech companies—including Cisco, Apple, Intel, and McAfee—from its list of authorized brands.[84] The obvious results of such decisions have been economic ripple effects outside of China. For example, Cisco and IBM both recorded sales declines as China shifted to purchasing the Chinese counterparts to American technology products.[85]

Operationalizing the Framework: Conducting a Ripple Effects Assessment

As the examples described above indicate, the ripple effects of encryption policies can be challenging to map. Even more challenging is *anticipating* the exact ripple effects that propagate from any single encryption policy. At any given moment, several (sometimes competing) forces are at play, shaping and complicating the ripple effects. Nonetheless, the conceptual framework described above offers a starting place for policy-makers to think more systematically about the specific tools of a given encryption policy, the pathways that policy might activate, and the most likely effects of those interactions. In order to operationalize this framework, below we identify a variety of factors policy-makers should consider when trying to assess potential ripple effects of a proposed policy. By weighing and considering these factors, policy-makers can develop a more nuanced assessment of the probable ripple effects of a proposed policy.

The factors that follow are designed to help guide policy-makers to think more systematically about the potential effects of a proposed policy. To that end, we grouped the factors into five thematic clusters: (1) those relating to the political environment in a potentially affected country;[86] (2) those relating to the private sector in that potentially affected country; (3) those relating to the relationship between a country enacting the encryption policy and the potentially affected country; (4) those relating to the proposed policy itself; and (5) additional factors that may shape the ripple effects. Overall, we expect that these factors may be most useful to public policy decision-makers, but they may also help the private sector anticipate ripple effects that could affect industry and business.

Factors Relating to the Political Context in the Potentially Affected Country

- The encryption policies that the potentially affected country already has in place.
- The extent to which existing policies are entrenched within the country's political and legal system.
- The extent to which those policies are malleable and open to debate or internal or external influence.
- The extent to which consensus exists within the country around the use of encryption and how such policies relate to broader national industrial policies.
- The existence of political alliances that could enhance the ripple effects from another country's encryption policy.
- The existence of political alliances that could inhibit the ripple effects from another country's encryption policy.
- The legal and treaty obligations binding the potentially affected country that could enhance or inhibit the impact of another country's encryption policies.
- The extent to which the government of the potentially affected country has successfully invoked the "public good" as a rationale in both public debates and as a means of influencing private sector behavior.

Factors Relating to the Private Sector in the Potentially Affected Country

- The steps that the potentially affected country has taken to enhance the competitiveness of its domestic private industries, particularly in the sectors affected by the proposed encryption policy.
- The relationship between the public and private sectors in the potentially affected country, particularly with respect to how both encryption policies and technologies are developed.
- The amount of human and technological resources within the private sector of the potentially affected country sufficient to develop new encryption tools and the extent to which the country wants to develop those resources further through policy.
- The ways in which the private sector in the potentially affected country might respond to the encryption policy.

Factors Relating to the Relationship between the Two Countries

- The overall nature of the relationship between the originating country and the potentially affected country.
- The degree to which the originating country wields hegemonic, political, economic, and/or soft power over the potentially affected country.
- The extent to which the originating country wields particular influence over the potentially affected country in the domains affected by the encryption policy.
- The manner in which the media in the potentially affected country report on the originating country and/or the country's encryption policies.
- The manner in which the media in the potentially affected country have previously reported on the originating country's policies.
- The degree to which the private sector in the potentially affected country is dependent on encryption technology from, or sales to, the originating country.
- The degree to which the public sector in the potentially affected country is dependent on encryption technology from, or sales to, the originating country.

Factors Relating to the Proposed Encryption Policy

- The clarity of the drafting and intent of the originating country's encryption policy.
- The degree to which implementation of the encryption policy could change over time.
- The potential for others to misinterpret the originating country's encryption policy.

Additional Factors That May Shape the Ripple Effects

- The level of involvement and influence of civil society groups within the potentially affected country.
- The position of those civil society groups on the encryption policy and their ability to influence the debate within the potentially affected country on that policy.
- The compatibility between the encryption policy and international standards or norms relating to encryption or technology policy.

This non-exhaustive list of factors can provide a lattice around which policy-makers can build a more comprehensive understanding of potential ripple effects. The factors do not in themselves offer any easy answers. In fact, each will require careful research and analysis, and then the factors must be carefully weighed and evaluated together. They represent only a first step. Evaluating these factors can help policy-makers begin to more clearly understand and anticipate potential ripple effects, improving the quality of informed decision-making. Indeed, over time, as these factors are further refined and developed, they may even assist policy-makers in managing ripple effects.

Conclusion

This paper offers a conceptual framework that can help policy-makers better understand and anticipate the potential international ripple effects of domestic encryption policies. Through the use of the factors identified above, policy-makers can engage in more informed decision-making by carefully and systematically thinking through the various instruments of encryption policy-making, the relationships and pathways those instruments can activate, and the range of effects that might emerge. Our framework can be a useful starting place, but in an effort to make these ripple effects more comprehensible, it also oversimplifies. Often, encryption policies are considered in parallel both with each other and with changing world events, leading to a range of interference patterns and feedback loops as the ripple effects propagate outwards. Future work in this space may help refine and add additional nuance to our framework and factors as we continue to research the full scope and impact of encryption policies.

NOTES

1 Evan Perez and Tim Hume, "Apple Opposes Judge's Order to Hack San Bernardino Shooter's iPhone," *CNN*, February 18, 2016, accessed February 15, 2018, https://www.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple.

2 Ellen Nakashima, "FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone," *Washington Post*, April 12, 2016, accessed February 15, 2018, https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?utm_term=.7b76bbaf64a7; Laurie Segall, Jose Pagliery, and Jackie Wattles, "FBI Says It Has Cracked Terrorist's iPhone Without Apple's Help," *CNN Money*, March 29, 2016, accessed February 15, 2018, http://money.cnn.com/2016/03/28/news/companies/fbi-apple-iphone-case-cracked/index.html.

3 Dustin Volz and Mark Hosenball, "Leak of Senate Encryption Bill Prompts Swift Backlash," *Reuters*, April 8, 2016, accessed February 15, 2018, https://www.reuters.com/article/us-apple-encryption-legislation/leak-of-senate-encryption-bill-prompts-swift-backlash-idUSKCN0X52CG.

4 Spencer Ackerman, "Apple Encryption Case Risks Influencing Russia and China, Privacy Experts Say," *The Guardian*, February 17, 2016, accessed February 15, 2018, https://www.theguardian.com/technology/2016/feb/17/apple-fbi-encryption-san-bernardino-russia-china; Matt Olsen, Bruce Schneier, and Jonathan Zittrain, "Don't Panic: Making Progress on the 'Going Dark' Debate,"Berkman Klein Center for Internet & Society, February 1, 2016, 9, ("However, if the U.S. government were to mandate architectural changes, surveillance would be made easier

for both the U.S. government and foreign governments, including autocratic regimes known to crack down on political dissidents."), accessed February 15, 2018, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

5 Devlin Barrett and Ellen Nakashima, "Texas Gunman's iPhone Could Reignite FBI-Apple Feud over Encryption," *Washington Post*, November 8, 2017, accessed February 15, 2018, https://www.washingtonpost.com/world/national-security/texas-gunmans-iphone-could-reignite-fbi-apple-feud-over-encryption/2017/11/08/0c2b3eb6-c48f-11e7-aae0-cb18a8c29c65_story.html?utm_term=.5ccb27745cf0; Jon Brodkin, "Trump's DOJ Tries to Rebrand Weakened Encryption as 'Responsible Encryption,'" *Ars Technica*, October 10, 2017, accessed February 15, 2018, https://arstechnica.com/tech-policy/2017/10/trumps-doj-tries-to-rebrand-weakened-encryption-as-responsible-encryption.

6 Our broad definition is not unique. For example, one scholar looked at a range of government actions that affected encryption use across human rights, law enforcement, intelligence, trade and export controls. See Ashley Deeks, "The International Legal Dynamics of Encryption," Hoover Institution, October 11, 2016, accessed February 15, 2018, https://www.hoover.org/research/international-legal-dynamics-encryption; see also Richard Cowan, "U.S. Tech Industry Appeals to Obama to Keep Hands Off Encryption," *Reuters*, June 8, 2015, accessed February 15, 2018, https://www.reuters.com/article/us-cybersecurity-usa-encryption-idUSKBN0OP09R20150609. Article quotes US technology companies in a letter to President Obama, stating, "We are opposed to *any policy actions or measures* that would undermine encryption as an available and effective tool (emphasis added)."

7 Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar, "A Worldwide Survey of Encryption Products," Berkman Klein Center for Internet & Society, February 11, 2016, accessed February 15, 2018, https://cyber.law.harvard.edu/publications/2016/encryption_survey.

8 Of course, domestic encryption policies are often shaped by, or in reaction to, a variety of forces, both domestic and international. We highlight some of these feedback loops in our examples.

9 Steven Levy, "Battle of the Clipper Chip," *New York Times*, June 12, 1994, accessed February 15, 2018, https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html; Neil Richards and Woodrow Hartzog, "Apple v the FBI: Why the 1789 All Writs Act is the Wrong Tool," *The Guardian*, February 24, 2016, accessed February 15, 2018, https://www.theguardian.com/technology/2016/feb/24/apple-v-the-fbi-why-1789-all-writs-act-is-the-wrong-tool.

10 Bruce Schneier, "NSA Plans for a Post-Quantum World," *Schneier on Security* (blog), August 21, 2015, accessed February 15, 2018, https://www.schneier.com/blog/archives/2015/08/nsa_plans_for_a.html.

11 "NSA's Prism: Few Options for Tech Companies to Defy US Intelligence Demands," *Reuters*, June 9, 2013, noting a lack of clarity about whether or not companies voluntarily participated in PRISM, accessed February 15, 2018, http://gadgets.ndtv.com/internet/news/nsas-prism-few-options-for-tech-companies-to-defy-us-intelligence-demands-377170.

12 "Law Enforcement Guidelines," Tumblr, accessed January 19, 2018, https://tumblr.zendesk.com/hc/en-us/articles/231925668-Law-Enforcement-Guidelines; Chance Miller, "Apple Agrees to Analyze Contents of iPhone Found in Boat of Missing Teens," *9 to 5 Mac*, April 30, 2016, accessed February 15, 2018, http://9to5mac.com/2016/04/30/apple-missing-florida-teens-iphone-boating-trip.

13 "List of Dual-Use Goods and Technologies and Munitions List," The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, April 4, 2016, accessed February 15, 2018, 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.

14 "NIST Cryptographic Standards and Guidelines Development Process," Cryptographic Technology Group, National Institute of Standards and Technology, March 2016, accessed February 15, 2018, http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7977.pdf.

15 "Edward Snowden: Leaks that Exposed US Spy Programme," *BBC News*, January 17, 2014, accessed February 15, 2018, http://www.bbc.com/news/world-us-canada-23123964.

16 Glenn Greenwald and Ewen MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others," *The Guardian*, June 7, 2013, accessed February 15, 2018, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

17 Greenwald and MacAskill, "NSA Prism Program."

18 Grant Gross, "Internet Infrastructure Groups Move Away from US Gov't Over Spying," *PCWorld*, October 16, 2013, accessed February 15, 2018, https://www.pcworld.com/article/2055240/internet-infrastructure-groups-move-away-from-us-govt-over-spying.htm.

19 Clint Boulton, "NSA's PRISM Could Cost IT Service Market $180 Billion," *Wall Street Journal*, August 16, 2013, accessed February 15, 2018, http://blogs.wsj.com/cio/2013/08/16/nsas-prism-could-cost-it-service-market-180-billion.

20 Bruce Schneier, "The Strange Story of Dual_EC_DRBG," *Schneier on Security* (blog), November 15, 2007, accessed February 15, 2018, https://www.schneier.com/blog/archives/2007/11/the_strange_sto.html.

21 Dan Goodin, "NSA Official: Support of Backdoored Dual_EC-DRBG Was 'Regrettable,'" *Ars Technica*, January 14, 2015, accessed February 15, 2018, http://arstechnica.com/security/2015/01/nsa-official-support-of-backdoored-dual_ec_drbg-was-regrettable.

22 Tom Simonite, "NSA Says It 'Must Act Now' Against the Quantum Computing Threat," *MIT Technology Review*, February 3, 2016, accessed February 15, 2018, https://www.technologyreview.com/s/600715/nsa-says-it-must-act-now-against-the-quantum-computing-threat.

23 Yochai Benkler, "We Cannot Trust Our Government, So We Must Trust The Technology," *The Guardian*, February 22, 2016, accessed February 15, 2018, https://www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi.

24 Cory Bennett, "Senate Encryption Bill Draft Mandates 'Technical Assistance,'" *The Hill*, April 7, 2016, accessed February 15, 2018, http://thehill.com/policy/cybersecurity/275567-senate-intel-encryption-bill-mandates-technical-assistance; David Meyer, "Here's Why Apple is Going to War Over FBI 'Backdoor' Order," *Fortune*, February 17, 2016, "Why the FBI Chose to Try the Apple Encryption Case in the Media," *Fast Company*, February 22, 2016, accessed February 15, 2018, https://www.fastcompany.com/3057033/why-the-fbi-chose-to-try-the-apple-encryption-case-in-the-media.

25 David Wright and Reinhard Kreissl, "European Responses to the Snowden Revelations: A Discussion Paper," Increasing Resilience in Surveillance Societies, December 2013, accessed February 15, 2018, http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf.

26 Daniel Severson, "Taking Stock of the Snoopers' Charter: The U.K.'s Investigatory Powers Bill," *Lawfare* (blog), March 14, 2016, accessed February 15, 2018, https://www.lawfareblog.com/taking-stock-snoopers-charter-uks-investigatory-powers-bill.

27 Daniel Severson, "The World's Not Waiting for California: France Moves to Enforce Decryption," *Lawfare* (blog), March 7, 2016, accessed February 15, 2018, https://www.lawfareblog.com/worlds-not-waiting-california-france-moves-enforce-decryption; Bhairav Acharya, Kevin Bankston, Russ Schulman, and Andi Wilson, "Deciphering the European Encryption Debate: France," *New America*, August 2017, accessed February 15, 2018, https://na-production.s3.amazonaws.com/documents/France_Paper_8_8.pdf; "French Parliament Rejects Data Localization Amendment," *Privacy & Information Security Law Blog*, Hunton & Williams, July 1, 2016, accessed February 15, 2018, https://www.huntonprivacyblog.com/2016/07/01/french-parliament-rejects-data-localization-amendment.

28 Christian Keszthelyi, "Hungarian Legislation Enables Encrypted Communication," *Budapest Business Journal*, May 12, 2016, accessed February 15, 2018, https://bbj.hu/politics/hungarian-legislation-enables-encrypted-communication_116019; Daniel Severson, "The Encryption Debate in Europe," Hoover Institution, March 21, 2017, accessed February 15, 2018, https://www.hoover.org/sites/default/files/research/docs/severson_webreadypdf.pdf.

29 Patrick Howell O'Neill, "Dutch Government Backs Strong Encryption, Condemns Backdoors," *The Daily Dot*, January 4, 2016, accessed February 15, 2018, https://www.dailydot.com/layer8/dutch-encryption-cabinet-backdoor.

30 Sara Zaske, "While US and UK Governments Oppose Encryption, Germany Promotes It. Why?" *ZDNet*, October 26, 2015, accessed February 15, 2018, http://www.zdnet.com/article/while-us-and-uk-govts-oppose-encryption-germany-promotes-it-why.

31 Adam Segal, "The Chinese Government Has its Eye on the FBI-Apple Battle" (blog), Council on Foreign Relations, March 14, 2016, accessed February 15, 2018, https://www.cfr.org/blog/chinese-government-has-its-eye-fbi-apple-battle; Katie Benner and Eric Lichtblau, "Tim Cook Opposes Order for Apple to Unlock iPhone, Setting Up Showdown," *New York Times*, February 17, 2016, accessed February 15, 2018, https://web.archive.org/web/20160217141406/http:/www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.

32 "China Releases Draft Encryption Law for Public Comment," Covington & Burling LLP, May 2017, accessed February 15, 2018, https://www.cov.com/-/media/files/corporate/publications/2017/05/china_releases_draft_encryption_law_for_public_comment.pdf.

33 Luís Osvaldo Grossmann, "Brasil Abandona Padrão de Criptografia Maculado pela NSA," *Convergência Digital*, May 27, 2014, accessed February 15, 2018, http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=36860.

34 Luís Osvaldo Grossmann, "Abandonada Criptografia dos EUA, Brasil Passa a Usar Sistema Alemão," *Convergência Digital*, April 13, 2015, accessed February 15, 2018, http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=39368&sid=18.

35 Lisandra Paraguassu, "Abin Cria Sistemas de Criptografia para Proteger Dados do Governo," *O Estado de São Paulo*, September 7, 2013, accessed February 15, 2018, http://politica.estadao.com.br/noticias/geral,abin-cria-sistemas-de-criptografia-para-proteger-dados-do-governo,1072368.

36 "NSA After-Shocks: How Snowden Has Changed ICT Decision-makers' Approach to the Cloud," NTT Communications, 2014, accessed February 15, 2018, http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC_Report_WEB.pdf.

37 Isabelle de Pommereau, "In Snowden's Wake, Crypto-Startups Take Root in Germany," *Christian Science Monitor*, August 3, 2015, accessed February 15, 2018, https://www.csmonitor.com/World/Passcode/2015/0803/In-Snowden-s-wake-crypto-startups-take-root-in-Germany.

38 M. Rochan, "Snowden NSA Leaks: India's Election Commission Dumps Google," *International Business Times*, January10, 2014, accessed February 15, 2018, http://www.ibtimes.co.uk/snowden-nsa-leaks-indias-election-commission-dumps-google-1431822.

39 Jerin Mathew, "Cisco's China Equipment Sales Dented by NSA Spying Scandal," *International Business Times*, July 1, 2014, accessed February 15, 2018, http://www.ibtimes.co.uk/cisco-china-sales-nsa-spying-scandal-522159.

40 Mike Wheatley, "Russia Unveils Homegrown PC Microprocessor Chips," *Russia Insider*, May 8, 2015, accessed February 15, 2018, http://russia-insider.com/en/business/russias-mcst-unveils-homegrown-pc-microprocessor-chips/ri6603; Nick Farrell, "Russians Want AMD and Intel Out," *TechEye*, June 23, 2014, http://www.techeye.net/chips/russians-want-amd-and-intel-out.

41 Anton Troianovski and Danny Yadron, "German Government Ends Verizon Contract," *Wall Street Journal*, June 26, 2014, accessed February 15, 2018, https://www.wsj.com/articles/german-government-ends-verizon-contract-1403802226.

42 Michael Birnbaum, Souad Mekhennet, and Ellen Nakashima, "Paris Attack Planners Used Encrypted Apps, Investigators Believe," *Washington Post*, December 17, 2015, accessed February 15, 2018, https://www.washingtonpost.com/world/europe/paris-attack-planners-used-encrypted-apps-investigators-believe/2015/12/17/e798d288-a4de-11e5-8318-bd8caed8c588_story.html?utm_term=.5db548a78962; Lizzie Dearden, "Khalid Masood: Supspected Isis Supporter Used WhatsApp Two Minutes before London Attack," *Independent*, March 27, 2017, accessed February 15, 2018, http://www.independent.co.uk/news/uk/home-news/khalid-masood-whatsapp-westminster-london-attack-parliament-message-isis-terror-network-contacts-a7649206.html.

43 Bhairav Acharya, Kevin Bankston, Russ Schulman, and Andi Wilson, "Deciphering the European Encryption Debate: United Kingdom," *New America*, June 2017, "How the IPA will be used by the government to compel operators to comply with these technical notices remains an open question," accessed February 15, 2018, https://na-production.s3.amazonaws.com/documents/Transatlantic_Encryption_UK__Final.pdf.

44 Ivana Kottasova and Samuel Burke, "U.K. Government Wants Access to WhatsApp Messages," *CNN Tech*, March 27, 2017, accessed February 15, 2018, http://money.cnn.com/2017/03/27/technology/whatsapp-encryption-london-attack/index.html.

45 Már Másson Maack, "EU plan could mean a backdoor into encrypted messaging apps like WhatsApp," *The Next Web*, March 31, 2017, accessed February 15, 2018, https://thenextweb.com/eu/2017/03/31/eu-plan-could-mean-a-backdoor-into-encrypted-messaging-apps-like-whatsapp/#; Cory Doctorow, "Germany's Proposed Anti-Cryptography Bill: Backdoors and Hack-Backs," *Boing Boing*, December 5, 2017, accessed February 15, 2018, https://boingboing.net/2017/12/05/thomas-de-maiziere.html; Amar Toor, "France and Germany Want Europe to Crack Down on Encryption," *The Verge*, April 24, 2016, accessed February 15, 2018, https://www.theverge.com/2016/8/24/12621834/france-germany-encryption-terorrism-eu-telegram.

46 Daniel Severson, "The Encryption Debate in Europe," Hoover Institution, March 21, 2017, accessed February 15, 2018, https://www.hoover.org/research/encryption-debate-europe.

47 Catherine Stupp, "EU to Propose New Rules Targeting Encrypted Apps in June," *Euractiv*, March 30, 2017, accessed February 15, 2018, https://www.euractiv.com/section/data-protection/news/eu-to-propose-new-rules-on-police-access-to-encrypted-data-in-june.

48 "Outcome of the 3546th Council Meeting: Justice and Home Affairs," *Council of the European Union*, June 8–9, 2017, 10, accessed February 15, 2018, http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf. There are also members within the European Union pushing for formal protections for encrypted communication. European Parliament, "Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC," European Parliament Committee on Civil Liberties, Justice and Home Affairs, October 20, 2017, accessed February 15, 2018, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0324+0+DOC+PDF+V0//EN.

49 European Commission, "Rules for the Protection of Personal Data Inside and Outside the EU," accessed February 15, 2018, http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm.

50 "The EU Continues to Influence Global Data Privacy Regulations," Mobile Ecosystem Forum (MEF), February 13, 2017, accessed February 15, 2018, http://mobileecosystemforum.com/2017/02/13/the-eu-continues-to-influence-global-data-privacy-regulations.

51 Adrian Bridgwater, "Veritas: EU Data Protection Laws to Affect All Global Firms," *Forbes*, May 25, 2016, accessed February 15, 2018, https://www.forbes.com/sites/adrianbridgwater/2016/05/25/veritas-eu-data-protection-laws-to-affect-all-global-firms/2/#4204b23c5a39.

52 "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," European Commission, July 2, 2013, accessed February 15, 2018, http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

53 European Commission, "Cybersecurity," September 19, 2017, accessed February 15, 2018, https://ec.europa.eu/digital-single-market/en/cybersecurity.

54 For an overview regarding the EU cybersecurity policy and potential further steps to secure a safe and open internet with measures against state surveillance, see Marietje Schaake and Mathias Vermeulen, "Towards a Values-based European Foreign Policy to Cybersecurity," *Journal of Cyber Policy* 1, no. 1, May 8, 2016: 75–84.

55 Information Technology Act, 2000, Ministry of Electronics and Information Technology, Government of India, accessed February 15, 2018, www.meity.gov.in/content/view-it-act-2000.

56 "Criticism Forces Government to Roll Back Its Draft Encryption Policy," *Indian Express*, September 23, 2015, accessed February 15, 2018, http://indianexpress.com/article/india/india-others/government-withdraws-draft-national-encryption-policy-after-furore.

57 Ellen Barry, "India Retracts Proposal on Encryption for Social Media Data after Outcry," *New York Times*, September 22, 2015, accessed February 15, 2018, https://www.nytimes.com/2015/09/23/world/asia/india-withdraws-social-media-data-proposal-after-outcry.html?_r=0.

58 "Draft National Encryption Policy," *Firstpost*, September 22, 2015, https://www.scribd.com/document/282239916/DRAFT-NATIONAL-ENCRYPTION-POLICY; Pankaj Doval, "Encryption Policy to Ensure Secure Environment for Govt, says Deity," *Times of India*, September 22, 2015, accessed February 15, 2018, http://timesofindia.indiatimes.com/tech/tech-news/Encryption-policy-to-ensure-secure-environment-for-govt-says-Deity/articleshow/49052799.cms.

59 Scott Brady, "Keeping Secrets: A Constitutional Examination of Encryption Regulation in the United States and India," *Indiana International and Comparative Law Review* 22, no. 2 (2012): 317–18; Anandita Singh Mankotia, "Government, BlackBerry End Dispute over Interception of BB Devices," *India Times*, July 10, 2013, accessed February 15, 2018, http://economictimes.indiatimes.com/industry/telecom/government-blackberry-end-dispute-over-interception-of-bb-devices/articleshow/20995830.cms.

60 Brady, "Keeping Secrets," and Mankotia, "Government, BlackBerry End Dispute."

61 Bhairav Acharya, "The Short-lived Adventure of India's Encryption Policy," Berkeley Information Privacy Law Association, December 1, 2015, accessed February 15, 2018, https://bipla.berkeley.edu/35; Itika Sharma Punit, "After BlackBerry and Google, It May Now Be WhatsApp's Turn to Annoy the Indian Government," *Quartz India*, April 6, 2016, accessed February 15, 2018, http://qz.com/656055/after-blackberry-and-google-it-may-now-be-whatsapps-turn-to-annoy-the-indian-government.

62 Jan Kourn and Brian Acton, "End-to-end Encryption," *WhatsApp Blog*, April 5, 2016, accessed February 15, 2018, https://blog.whatsapp.com/10000618/end-to-end-encryption; Andrew Griffin, "WhatsApp End-to-End Encryption Update Might Have Made Chat App Illegal in India," *Independent*, April 8, 2016, accessed February 15, 2018, http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-end-to-end-encryption-update-might-have-made-chat-app-illegal-in-india-a6974921.html.

63 Ministry of Communications & IT and Department of Telecommunications, Government of India, license agreement for provision of the internet, clause 2.2 (vii), accessed February 15, 2018, http://www.dot.gov.in/sites/default/files/DOC270613-013.pdf.

64 Indian Telegraph Act, 1885, Section 5(1), accessed February 15, 2018, http://www.dot.gov.in/actrules/indian-telegraph-act-1885.

65 Krishnadas Rajagopal, "No Ban on Whatsapp: Supreme Court," *The Hindu*, June 29, 2016, accessed February 15, 2018, http://www.thehindu.com/news/national/No-ban-on-Whatsapp-Supreme-Court/article14408732.ece.

66 Indo-Asian News Service, "WhatsApp in Over 109 Countries, with 70 Million Users in India: Study," *Gadgets 360*, May 26, 2016, accessed February 15, 2018, http://gadgets.ndtv.com/apps/news/whatsapp-in-over-109-countries-with-70-million-users-in-india-study-841858; Sneha Johari, "WhatsApp YouTube & Google Top 3 Apps by Daily Active Users: Jana Study," *Medianama*, March 11, 2016, accessed February 15, 2018, https://www.medianama.com/2016/03/223-most-used-apps-india-jana.

67 Andrea Peterson and Dom Phillips, "Brazil's Latest WhatsApp Ban Is Pushing Users to Other Encrypted Messaging Apps," *Washington Post*, May 3, 2016, accessed February 15, 2018, https://www.washingtonpost.com/news/the-switch/wp/2016/05/03/brazils-latest-whatsapp-ban-is-pushing-users-to-other-encrypted-messaging-apps.

68 "Russia: Country Report," Freedom House, 2015, 6, accessed February 15, 2018, https://freedomhouse.org/report/freedom-net/2015/russia.

69 "Russia's State Duma Just Approved Some of the Most Repressive Laws in Post-Soviet History," *Meduza*, June 24, 2016, accessed February 15, 2018, https://meduza.io/en/feature/2016/06/24/russia-s-state-duma-just-approved-some-of-the-most-repressive-laws-in-post-soviet-history.

70 Leonid Bershidsky, "Russia Wants to Make an Example of Telegram," *Bloomberg*, September 28, 2017, accessed February 15, 2018, https://www.bloomberg.com/view/articles/2017-09-28/russia-wants-to-make-an-example-of-telegram; "Russia Tells Facebook to Localize User Data or Be Blocked," *Reuters*, September 26, 2017, accessed February 15, 2018, https://www.reuters.com/article/us-russia-facebook/russia-tells-facebook-to-localize-user-data-or-be-blocked-idUSKCN1C11R5.

71 Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," *World Policy Journal,* Fall 2013, accessed February 15, 2018, http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.

72 Vinod Sreeharsha, "WhatsApp Blocked in Brazil as Judge Seeks Data," *New York Times*, May 2, 2016, accessed February 15, 2018, https://www.nytimes.com/2016/05/03/technology/judge-seeking-data-shuts-down-whatsapp-in-brazil.html.

73 Joon Ian Wong, "The Messaging App That's Benefiting from WhatsApp's Ban in Brazil," *Quartz*, May 3, 2016, accessed February 15, 2018, http://qz.com/675070/the-messaging-app-thats-benefiting-from-whatsapps-ban-in-brazil; Vlad Savov, "Brazil's WhatsApp Ban is Driving Millions of Users to Telegram," *The Verge*, December 17, 2015, accessed February 15, 2018, https://www.theverge.com/2015/12/17/10386776/brazil-whatsapp-ban-telegram-millions-users.

74 Cory Bennett, "China Tightens Internet Control with National Security Law," *The Hill*, July 1, 2015, accessed February 15, 2018, http://thehill.com/policy/cybersecurity/246628-china-tightens-internet-control-with-national-security-law.

75 Ben Blanchard, "China Passes Controversial Counter-Terrorism Law," *Reuters*, December 27, 2015, https://www.reuters.com/article/us-china-security-idUSKBN0tA07220151228.

76 Blanchard, "China Passes Controversial Counter-terrorism Law."

77 Kate Conger, "China's New Cybersecurity Law is Bad News for Business," *TechCrunch*, November 6, 2016, accessed February 15, 2018, https://techcrunch.com/2016/11/06/chinas-new-cybersecurity-law-is-bad-news-for-business.

78 "China Releases Draft Encryption Law for Public Comment," Covington & Burling LLP, May 9, 2017, accessed February 15, 2018, https://www.cov.com/-/media/files/corporate/publications/2017/05/china_releases_draft_encryption_law_for_public_comment.pdf.

79 Steve Lohr, "In 2015, Technology Shifts Accelerate and China Rules, IDC Predicts," *Bits* (blog), *New York Times*, December 2, 2014, accessed February 15, 2018, http://bits.blogs.nytimes.com/2014/12/02/in-2015-technology-shifts-accelerate-and-china-rules-idc-predicts.

80 Paul Mozur and Jane Perlez, "China Quietly Targets U.S. Tech Companies in Security Reviews," *New York Times*, May 16, 2016, accessed February 15, 2018, https://www.nytimes.com/2016/05/17/technology/china-quietly-targets-us-tech-companies-in-security-reviews.html.

81 John Shinal, "U.S. Shouldn't Emulate China's Encryption Policy," *USA Today*, June 9, 2015, accessed February 15, 2018, https://www.usatoday.com/story/tech/columnist/shinal/2015/06/09/alibaba-jack-ma-china-encryption-us-president-obama-facebook-twitter-google-hp/28753623.

82 Eva Dou and Rachael King, "China Sets New Tone in Drafting Cybersecurity Rules," *Wall Street Journal*, August 26, 2016, accessed February 15, 2018, https://www.wsj.com/articles/china-moves-to-ease-foreign-concerns-on-cybersecurity-controls-1472132575.

83 Paul Mozur, "Jitters in Tech World Over New Chinese Security Law," *New York Times*, July 2, 2015, accessed February 15, 2018, https://www.nytimes.com/2015/07/03/business/international/jitters-in-tech-world-over-new-chinese-security-law.html?_r=0; Katherine Koleski, "The 13th Five-Year Plan," U.S.-China Economic and Security Review Commission, Feb. 14, 2017, accessed February 15, 2018, https://www.uscc.gov/sites/default/files/Research/The%2013th%20Five-Year%20Plan_Final_2.14.17_Updated%20%28002%29.pdf.

84 Zack Whittaker, "It's Official: NSA Spying Is Hurting the US Tech Economy," *ZDNet*, February 25, 2015, accessed February 15, 2018, http://www.zdnet.com/article/another-reason-to-hate-the-nsa-china-is-backing-away-from-us-tech-brands.

85 Eva Dou and Juro Osawa, "China Aims to Build Its Own Secure Smartphones," *Wall Street Journal*, November 20, 2015, accessed February 15, 2018, https://www.wsj.com/articles/china-aims-to-build-its-own-secure-smartphones-1447961400.

86 These factors are intended to be universally applicable across geographies, and for that reason we use a flexible terminology that asks policy-makers to think about both their own proposed policy (the "originating country's encryption policy") and how it might affect each "potentially affected country."

The preferred citation for this publication is Ryan Budish, Herbert Burkert, and Urs Gasser, **Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects**, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1804 (February 28, 2018), available at https://lawfareblog.com/encryption-policy-and-its-international-impacts-framework-understanding-extraterritorial-ripple

About the Authors

RYAN BUDISH

Ryan Budish is an assistant research director at the Berkman Klein Center for Internet & Society at Harvard University. In this role, he has led several significant initiatives relating to cybersecurity, artificial intelligence, Internet censorship, surveillance, and multi-stakeholder governance mechanisms. He received his JD cum laude from Harvard Law School, where he was an editor of the *Harvard Law Review*.

HERBERT BURKERT

Herbert Burkert is the president of the Research Center for Information Law, University of St. Gallen, Switzerland. He has served as an advisor to national and regional governments as well as to international organizations. He has studied law, political science, and history at the University of Cologne (Germany) and the University of Dublin (Ireland).

URS GASSER

Urs Gasser is the executive director of the Berkman Klein Center for Internet & Society at Harvard University, where he co-leads the Ethics and Governance of AI initiative and serves as a professor of practice at Harvard Law School. His research and teaching focus on the interplay between law and technology. Gasser is a graduate of the University of St. Gallen and Harvard Law School.

Synopsis

This paper explores the potential international ripple effects that can occur following changes to domestic encryption policies. Whether these changes take the form of a single coherent national policy or a collection of independent (or even conflicting) policies, the impacts can be unexpected and wide-ranging. This paper offers a conceptual model for how the ripple effects from national encryption policies might propagate beyond national borders. And we provide a set of factors that can help policy-makers anticipate some of the most likely ripple effects of proposed encryption policies.

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