THE SPECTRUM OF ENCRYPTION
Safety and Security Considerations

AUTHORS
Lindsey R. Sheppard
Brian Katz
Kathleen H. Hicks
Joseph Federici

A Report of THE INTERNATIONAL SECURITY PROGRAM

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES
AUTHORS
Lindsey R. Sheppard
Brian Katz
Kathleen H. Hicks
Joseph Federici

A Report of THE INTERNATIONAL SECURITY PROGRAM
About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world’s greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS’s purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS’s values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS is ranked the number one think tank in the United States as well as the defense and national security center of excellence for 2016-2018 by the University of Pennsylvania’s “Global Go To Think Tank Index.”

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2020 by the Center for Strategic and International Studies. All rights reserved.
Acknowledgments

The authors are grateful to William Crumpler, Will Carter, and Jim Lewis for their research contributions on the encryption policy environments. We would also like to thank Suzanne Spaulding and Amy Lehr for their insights and feedback throughout the project. Thank you to Collett Preston for his support in the report drafting process. A special thanks to the CSIS iDeas Lab, including Rebecka Shirazi, Jeeah Lee, Sarah Grace, Jacque Schrag, Emily Tiemeyer, and Philip Meylan for their hard work on this report and related materials. Finally, the authors would like to thank those who participated in the workshops and one-on-one interviews. We greatly appreciate the time and knowledge they shared with us for this study.

CSIS received a financial gift from Facebook in support of research on encryption safety and security.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INTRODUCTION</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>METHODOLOGY</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>BACKGROUND</strong></td>
<td>4</td>
</tr>
<tr>
<td>Uses and Applications</td>
<td>4</td>
</tr>
<tr>
<td>Priorities and Considerations</td>
<td>5</td>
</tr>
<tr>
<td><strong>ENCRYPTION POLICY ENVIRONMENTS</strong></td>
<td>7</td>
</tr>
<tr>
<td>Environment 1: Design Mandates</td>
<td>7</td>
</tr>
<tr>
<td>Environment 2: Technology-neutral Access Mandates</td>
<td>8</td>
</tr>
<tr>
<td>Environment 3: User Decryption Mandates</td>
<td>8</td>
</tr>
<tr>
<td>Environment 4: Workarounds to Access Encrypted Data</td>
<td>8</td>
</tr>
<tr>
<td>Environment 5: No Access to Encrypted Communications</td>
<td>9</td>
</tr>
<tr>
<td><strong>USER COMMUNITIES</strong></td>
<td>11</td>
</tr>
<tr>
<td>Independent Voices</td>
<td>12</td>
</tr>
<tr>
<td>At-risk Groups</td>
<td>14</td>
</tr>
<tr>
<td>Businesses and Organizations</td>
<td>15</td>
</tr>
<tr>
<td>Foreign Policy</td>
<td>18</td>
</tr>
<tr>
<td>Terrorists, Extremists, and Hate Groups</td>
<td>20</td>
</tr>
<tr>
<td><strong>SUMMARY FINDINGS</strong></td>
<td>24</td>
</tr>
<tr>
<td><strong>CONCLUSION</strong></td>
<td>31</td>
</tr>
<tr>
<td><strong>ABOUT THE AUTHORS</strong></td>
<td>33</td>
</tr>
</tbody>
</table>
In May 2020, China announced a new national security law for Hong Kong aimed at imposing restrictions on criticizing the Chinese Communist Party (CCP) government already in place in mainland China. With the prospect of digital free speech under fire, and the likelihood of surveillance by the CCP, demand for virtual private network (VPN) services skyrocketed in Hong Kong overnight. The drive for VPNs directly reflected the desire to evade this threat of digital authoritarianism using an approach that would encrypt data and send it through servers outside of China.

At almost the same time and halfway around the world, an assailant linked to a right-wing extremist group killed a security officer outside a federal courthouse. The murder followed months of reporting that the group, which calls itself the Boogaloo Boys, was angered by the Black Lives Matter movement and by stay-at-home rules necessitated by the Covid-19 pandemic. The group has been using encrypted email to communicate plans for violence.
Encryption technology plays a role in both these stories. There are many types and applications of encryption. It is used for everything from preventing illicit access to data on devices to protecting communications in transit and authenticating financial transactions. In the past, most commercially available encryption allowed the service provider, whether a device maker, operating system (OS) provider, app company, or telecommunications provider, to decrypt users’ data or communications (called “recoverable encryption”). Service providers use those access mechanisms to help users recover their accounts if they forget their passwords, to enable communication between platforms with different security protocols, and to mine user data to target advertising. Today, however, both major OS families (Android and iOS) and a growing number of instant messaging companies have implemented unrecoverable encryption which can only be accessed with the user’s private key, securing both data in transit and data at rest.

Policymakers in the United States and other democratic countries face several dilemmas related to the use of encryption. To date, most attention has focused on one issue in particular: the so-called “Going Dark” problem. This refers to forms of encryption that protect devices and communications in ways that make it difficult or impossible for law enforcement and security agencies to access that data. As the Boogaloo Boys example demonstrates, the importance of digital evidence is growing as more of daily life moves online. Many countries are unwilling to accept a future in which they will have no way to access these sources of information. In October 2019, U.S. Attorney General William Barr, Australian Home Minister Peter Dutton, and UK Home Secretary Priti Patel released an open letter urging Facebook to delay its plans to implement encryption across its platform that would deny law enforcement access to data to support its investigations. Interpol has also been considering whether to condemn the spread of unrecoverable encryption.

Yet as the Hong Kong example demonstrates, democracies also share a concern about protecting individual freedoms and other user needs. Residents and businesses in countries such as Russia and China are increasingly subjected to limitations on encryption that exceed defensible needs of law enforcement and instead support the goals of autocracy.

Finally, federal and state lawmakers must consider the implications of global encryption policies on U.S. persons, organizations, and businesses whose travels or operations span national borders. The United States has a role to play in setting norms and standards relating to encryption policy in order to advance the economic viability of U.S. companies, the rights of its citizens traveling or working abroad, and the protection of civic space for American charitable and non-profit organizations.

How the United States and other governments choose to maintain lawful access to digital content will define the technology ecosystem in which companies operate and the forms and applications of encryption to which their citizens will have access. Users in advanced democracies have different needs and make different uses of encryption than vulnerable populations living under repressive regimes, but the choices countries make about encryption policies will have implications beyond their own borders and their own circumstances. How different countries address the question of access to encryption will shape how global companies build their products, which will have significant implications for the tools and choices available to a wide range of users around the world.

The business, legal, and national security communities in the United States must grapple with all of these dimensions of encryption policy. This CSIS study explores these issues through the lens of key encryption user groups, their governments, and U.S. values and interests. Its findings illuminate the central trade-offs policymakers face and demonstrate that decisions surrounding when, where, how, and by whom encryption is used should be more nuanced than an all-or-nothing approach.
Methodology

Several key and interrelated questions motivated CSIS’s efforts over the nine-month course of this study: Why is encryption particularly important for the various communities included in this study? How do these groups use encryption for both devices and communications? Which perspectives are most relevant and are the main priorities? And finally, what are the impacts and implications (e.g., challenges, costs, benefits) of various policy environments?

Research proceeded in three major phases. In its first phase, the team identified and assessed five broad categories of encryption policy environments that current and emerging governments use around the world. These policies include:

- Design mandates for encryption;
- Technology-neutral access mandates to encrypted data;
- User decryption mandates;
- Workarounds to access encrypted data; and
- No access to encrypted communications

The study team next sought to build off the extant body of research focusing on law enforcement challenges posed by criminal and terrorist use of encryption by expanding the analytic field of view to include a broader range of encryption users. Journalists, marginalized groups, and ordinary people, for instance, are important consumers of encryption technology. In all, CSIS assessed the encryption approaches employed by five types of users in the above policy environments:

- Independent voices, including journalists, activists, dissidents, civil society, and non-governmental organizations (NGOs);
- At-risk users, including those marginalized based on their race, gender, ethnicity, sexual orientation, or other forms of identity;
- U.S.-based businesses;
- U.S. foreign policy practitioners, such as diplomats and military and intelligence officers; and
- Terrorists, extremists, and hate groups.

In its final phase, the CSIS team refined the insights it gleaned from its research, focusing on findings of greatest importance to U.S. policymakers. Understanding the perspectives of the five user groups, government perspectives about each group, and U.S. government principles and responsibilities ensured a firm foundation for the team’s findings.

In addition to traditional primary- and secondary-source research, the study team convened expert workshops at critical points during its effort to vet its approach and examine emerging findings. CSIS researchers also conducted approximately 10 not-for-attribution interviews with a range of stakeholders (in privacy, security, and safety), technical experts, and user communities to support the research effort.
Encryption is a critical tool to protect sensitive information, prevent cybercrime and digital fraud, and authenticate digital transactions. For vulnerable groups, both recoverable and unrecoverable encryption can be an essential means to protect communications and activities from repressive regimes, criminals, hate groups, and other bad actors. But malicious actors can also utilize encryption to hide their activities from law enforcement and security agencies.10

Uses and Applications
Encryption serves a variety of purposes for individuals, governments, and organizations in protecting their data and information, whether “at rest” when stored on computers, smartphones, and other devices or “in transit” in communications between users, devices, and applications.11 For data “in transit,” encryption has long played a critical role in protecting the security and secrecy of communications, particularly for governments and militaries.
is a key feature of user communications, whether integrated into the hardware and software on their devices, the secure web browsers and VPNs many use in accessing the internet, or the applications on smartphones, laptops, or other devices used to communicate. The applications of encryption are as varied as its users and their interests, but several uses of unrecoverable encryption—communications and mobile device storage—are of particular importance for the user communities in this study.

**Person-to-person Communication:**
Encrypted messenger apps such as WhatsApp, Signal, Telegram, and Messenger allow users to communicate instantly and relatively securely around the globe, for both personal and professional use. Instant messaging apps and encrypted email services such as ProtonMail are often selected because of their end-to-end encryption to safeguard against monitoring as well as other communication features such as secure voice calls.

**Groups and Community Building:**
The group chat feature offered by many encrypted instant messenger apps provides all types of groups and communities—from friends and families to organizations and interest groups—the ability to communicate and connect continuously with fellow members, both within and across global borders.

**Broadcasting and Information Dissemination:**
Encrypted communications apps can function as broadcasting channels for the instant dissemination of information to hundreds or even thousands of users. Radio, broadcast list, and public channel features on commercial apps can be used to share important information among citizens, such as emergency alerts for crime and natural disasters, but can also propagate the spread of misinformation and disinformation.

**Coordination and Mobilization:**
Secure messaging enables users and groups to plan, coordinate, and execute tasks and operations across geographic areas and to mobilize members for specific courses of action, be it orchestrating protests, coordinating business trips, or—concerningly—conspiring to conduct terrorist attacks.

**Content Sharing:**
Along with instant messaging and broadcast dissemination, encryption can be used to securely store and share photos, videos, documents, and other digital material via messenger apps, online cloud sharing, and digital “drop boxes.”

**Commerce and Financial Transactions:**
Encrypted peer-to-peer (P2P) payment platforms enable direct and secure payments, money transfers, and commercial transactions between users and organizations.

### Priorities and Considerations

User communities, policymakers, and other relevant stakeholders in the encryption debate hold a variety of priorities, concerns, and objectives in considering encryption policies and their implications. Rather than existing in isolation or conflict, these considerations and priorities often overlap, as users and governments weigh the costs and benefits of various encryption options for privacy, cybersecurity, public safety, and national security.

**Privacy:**
Users who prioritize privacy view encryption as critical in preventing technology companies and third parties from monitoring and disclosing data and in protecting communications from state surveillance and other government overreach. Advocates believe encryption of data and devices has become an intrinsic part of the right to privacy, free speech, civil liberties, and even human rights, particularly for users living under authoritarian regimes, where censorship, oppression, and monitoring of communications can put them at risk. Organizations and businesses similarly have roles in safeguarding user privacy in the digital era.
**Cybersecurity:** From a cybersecurity perspective, encryption should be optimized or even maximized to ensure the safeguarding of data, communications, devices, and hardware from an array of threat actors, including cybercriminals, hacktivists, commercial hacking companies, and foreign espionage.\(^2\) Cybersecurity proponents focus in particular on protecting the confidentiality, integrity, and availability of data from theft and manipulation, be it for critical public- and private-sector infrastructure or for individual businesses and citizens.\(^2\)

**Public Safety:** In terms of public safety, protecting citizens from crime, misinformation, threats, and violence and enabling law enforcement to investigate and prevent crimes and attacks is the top priority. For example, encryption protects dispatch communications for first responders and secures both attorney-client communications and sensitive legal case data. Encryption may provide both benefits and obstacles to achieving public safety objectives.\(^2\) From a public safety perspective, a key consideration is how end-to-end encryption for communications and full disk encryption on devices can disrupt or deny access for law enforcement to information and potential evidence to stop, solve, and prosecute offenses.\(^2\)

**National Security:** Related to but different from public safety, encryption can also be seen through the lens of national security and its implications for countering or enabling foreign intelligence collection, terrorist threats, and disinformation campaigns against a government and its citizens both domestically and worldwide.\(^2\)
The global encryption policy landscape is fracturing, with different countries pursuing different approaches to encryption through both legal and technical means. Encryption policies around the world can be broken into five broad categories. These approaches are not mutually exclusive, and many countries are pursuing a combination of these policies. Additionally, countries may pursue varying options to address the use of unrecoverable encryption for data at rest and data in transit. Some countries may choose to address one or the other, while others may formulate policies to address both.26

ENVIRONMENT 1
Design Mandates

At one end of the spectrum of policy options are laws and regulations that require companies to build their products and services in specific ways to facilitate access to data. Russia and China, for example, impose strict design mandates on companies outlining how
their products and services should be built, including the use of specific types of encryption.

Design mandates, often operationalized through certification, licensing, or testing regimes, can be built to ensure that only accessible encryption systems would be allowed in a country. Russia, for instance, requires providers of electronic communications services to “include in the apparatus additional hardware and software and create other conditions required by federal security service organs” to ensure their access to users’ data and forward the content of communications to security services upon request. In China, service providers are required to provide “technical interfaces, decryption, and other technical support assistance” through the country’s 2015 Counter-terrorism law. China’s 2019 Encryption Law also clarifies that all encryption affecting national security or national welfare must abide by China’s testing and certification regime, which will almost certainly require the use of state-certified and state-accessible encryption standards.

**ENVIRONMENT 2**

**Technology-neutral Access Mandates**

Technology-neutral mandates refrain from specifying how technology providers must build their systems but still require companies to provide decrypted data when asked by the government. France, for example, requires encryption providers to deliver the means to decrypt data within 72 hours or face two years of imprisonment and a fine of 150,000 euros. Though in this environment technology companies are left with the flexibility to decide how access is accomplished, the end effect is the same as in the case of design mandates: only providers who are willing and able to provide decrypted data to the government can operate legally in the country.

Some countries have passed laws that could allow them to mandate recoverability but have yet to enact them, and the exact scope of those authorities remains unclear. The United Kingdom and Australia have both recently passed laws that arguably give their governments the authority to demand that companies maintain the capability to facilitate access to encrypted data. Despite the presence of these authorities, there is no public evidence that either government has actually used them to require companies to use recoverable encryption. This has led to a unique policy environment, as both technology companies and their users have been forced to adapt to an uncertain enforcement regime.

**ENVIRONMENT 3**

**User Decryption Mandates**

Some countries have addressed the challenge of encryption by requiring users to facilitate access to communications. Instead of compelling companies to facilitate access to their customers’ data, countries such as Australia and France can compel users to disclose their private encryption keys, including passwords and biometric keys such as fingerprints or face scans. U.S. law is murky on this subject. Users cannot be compelled to disclose their passwords, as these are treated as protected speech, but some courts have upheld the controversial practice of forcing criminal suspects to unlock encrypted data by providing biometric keys, for example, forcibly placing a suspect’s finger on a fingerprint scanner.

User mandates avoid imposing constraints on companies that provide encrypted products and services but require informing users that their data is being collected, often a problem in ongoing investigations. Furthermore, criminals and terrorists may choose to take the penalties associated with refusing to disclose their encryption keys instead of facing the much more serious consequences of revealing encrypted evidence of serious crimes.

**ENVIRONMENT 4**

**Workarounds to Access Encrypted Data**

Some governments have responded to the problem of “Going Dark” by expanding the use of workarounds to access encrypted systems rather than restricting access to encryption. These range from
lawful hacking and “man-in-the-middle” attacks to GCHQ’s (the United Kingdom’s signals intelligence agency) “ghost key” proposal, in which companies would surreptitiously add users to chats without notifying the other chatters. Some countries develop in-house capabilities in their law enforcement and security agencies to do lawful hacking, while others turn to vendors to buy hacking products and services, fueling the growth of “gray market” cyber companies whose activities tend to be in legal and ethical gray areas.

Germany has worked to foster its law enforcement’s ability to engage in lawful hacking to ensure that the spread of strong encryption does not impact public safety and security. In 2015, for example, German police hacked into the Telegram accounts of eight suspected right-wing extremists to access their encrypted communications and log new messages in real time. In 2017, lawful hacking authorities were formalized by a new law that explicitly authorized police to install malware on digital devices. The next year, Germany’s Ministry of the Interior created a new division on cyber and IT security that consolidated codebreaking operations to help support lawful hacking for police and intelligence agencies. Germany’s approach is now being copied by others, such as Sweden, who recently announced that it would grant its own law enforcement agencies similar powers to deploy spyware on suspects’ devices.

**ENVIRONMENT 5**

**No Access to Encrypted Communications**

Finally, some countries have no authorities in place to access encrypted communications. Countries may actively choose not to pursue authorities to access encrypted communications or may be unable to legislate accordingly. For advocates of encryption, this allows companies to maintain their privacy compact with users, while law enforcement and security authorities can use other sources of data, for example, metadata and data from IoT devices that are increasingly ubiquitous.

The United States is an example of this environment, with no existing authorities allowing government officials to demand accessibility and a limited and uncoordinated approach to lawful hacking. For law enforcement, this environment poses the greatest challenge. Though some countries may have the resources to support isolated attempts at leveraging technical workarounds, for most, certain types of data and communications will be effectively off-limits. The effectiveness of law enforcement operations will inevitably be compromised to varying degrees in the absence of this digital content, forcing agencies to rely more heavily on unencrypted data sources and other more traditional methods of evidence gathering.

**The Scope of Legal Authorities over Encryption Is Unclear in Some Countries**

The uncertain legal environment around encryption in many countries represents a growing challenge for companies. For example, under Australia’s 2018 Assistance and Access Bill, government agencies are empowered to issue compulsory “technical capability notices” (TCNs) requiring communications providers to build access mechanisms to provide access to data for law enforcement. According to the bill, these notices can be used to demand that providers modify their services and remove encryption they have applied. However, the bill also states that TCNs cannot be used to ask providers to “implement or build a systemic weakness . . . into a form of electronic protection . . . implement or build a new decryption capability . . . [or] render systemic methods of authentication or encryption less effective.” While this may seem to prevent the use of TCNs to restrict access to unrecoverable encryption, some are concerned that the lack of specificity over what constitutes a “systemic weakness” could allow the Australian government to use this authority to force companies to compromise the security of their products and services.
Similarly, in the United Kingdom the 2016 Investigatory Powers Act gave law enforcement agencies the authority to order operators to remove any “electronic protection applied by or on behalf of that operator to any communications or data.” While the bill limits these requests to those considered “proportionate” which “take into account the technical feasibility, and likely cost, of complying with those obligations,” officials have nonetheless continued to entertain the idea of using the authorities in the bill to force companies to remove end-to-end encryption. The United Kingdom’s GCHQ has already put forth a proposal for a system they believe would walk this tightrope between the bill’s authorities and its restrictions, based around the idea of secretly inserting the government into ongoing encrypted communications rather than breaking the encryption itself.

In India there is a wide divergence between the government’s written legal authorities over encryption and the reality of policies implemented on the ground. India’s IT Act of 2008 requires communications providers to assist in decrypting information at the request of law enforcement and authorizes the government to “prescribe the modes or methods for encryption.” Regulations by India’s Department of Communications require that any encryption provider using greater than 40-bit encryption reach an agreement with the government and disclose encryption keys before operating in the country. In reality, however, 40-bit encryption is largely obsolete, and services such as WhatsApp openly use 256-bit encryption keys and unrecoverable encryption. While WhatsApp has not yet been banned or forced to turn over its keys, it has been facing increasing pressure from the Indian government for failing to turn over data in response to law enforcement requests.

The lack of clarity around the extent of these authorities and how they are used means that, on one hand, companies face significant regulatory uncertainty around their obligations to disclose data. Foreign companies, in particular, could face inconsistent application or arbitrary enforcement of these laws. On the other hand, users in these countries may not trust the security of these platforms. For example, Apple claims that it does not modify its operating system for Chinese users, but Chinese Apple users might reasonably question whether the Chinese government can access their private data.
The user communities in this study characterize the driving user groups with respect to encryption policy and usage. The study team recognizes that average, everyday users have interests and needs in using encryption. Ordinary people are daily users and consumers of encryption and secure communications products. However, this study focuses on a subset of user communities that, taken together, illuminate the trade-offs inherent in encryption policy choices. These five user groups are as follows: independent voices; at-risk groups; businesses and organizations; foreign policy; and terrorists, extremists, and hate groups. The study team’s taxonomy is fluid, as individuals and organizations can move across these categories at different times based on circumstance or their own personal or professional choices. For each user community, the study team presents the user experience with respect to encryption applications and priorities and then summarizes the implications of different policy environments for the user.
INDEPENDENT VOICES

The independent voices user community focuses on those individuals and organizations whose views and activities remain independent from entities such as governments, governmental bodies, and corporations. The user community includes journalists, activists, dissidents, civil society, and non-governmental organizations (NGOs). Many of these users adopt a cybersecurity posture that uses encryption due to their professional or political circumstances, often dependent on geopolitical and personal security realities directly impacting them and relevant stakeholders. Particularly for journalists reporting on national security and intelligence or those reporting from within war zones and repressive regimes, encryption is often cited an enabler of and necessary tool for journalism. Globally, activists, political dissidents, and human rights defenders use encryption to protect themselves while they organize and operate in the face of repressive regimes, as digital communications can reveal sensitive information. Even in friendlier environments, independent voices use encryption to protect against surveillance, theft, and compromising data in areas such as borders, where legal rights may be murky. However, for those who largely come from non-technical or security backgrounds, many users observe a gap in the acknowledgement of the criticality of encryption and its actual use and implementation.

USER APPLICATIONS

Person-to-person Communication: The importance of encryption to independent voices is clear in the need to protect person-to-person communications. Journalists rely on encrypted communications for a variety of uses: to keep sources, conversations, and transcriptions confidential and secure; to protect devices with digital recordings and transcriptions of conversations; and to safeguard communications with colleagues and security teams. However, professionals in journalism, NGOs, and civil society interviewed for this research effort observed that use of encryption is uneven throughout the independent voices community despite its broad applicability. Users working on sensitive issues such as national security, intelligence, and armed conflict or those whose activities are based in less permissive regions such as warzones or highly repressive societies are more likely to proactively take steps to secure their digital footprint and data.

Content Sharing: The use of encryption to enable secure content sharing has been an important aspect of operations and cross-border collaboration for organizations and individuals. Journalists, news organizations, and NGOs make use of tools such as SecureDrop, a service that enables the secure and anonymous transfer of files, to safely communicate with sources and receive documents. Journalistic collaborations such as the Organized Crime and Corruption Project, which instigated the release of the Panama Papers, rely heavily on the secure storage and sharing of data, tools, and communications.

Coordination and Mobilization: For activists and dissidents, organization and mobilization for protest movements occur online, often through encrypted messaging services. While the 2019 protests in Hong Kong are noted for their reliance on encrypted applications for leaderless mobilization, CSIS research on mass protests notes that most movements in 2019 relied on encrypted messaging. Signal, WhatsApp, and Telegram were noted for their enabling role in the coordination and mobilization of mass protest movements. These digitally enabled protest movements...
reduce individual risk and make participation more likely when individuals believe they can anonymously engage.\textsuperscript{50} However, individuals inexperienced in maintaining a secure digital profile before the protest movement risk compromise in other vectors despite the content of messages being securely encrypted.

**PRIORITIES AND CONSIDERATIONS**

Of the broad priorities and considerations highlighted previously, the independent voices user community prioritizes cybersecurity and digital privacy as an enabler of their personal and professional safety and security. There is a heavy focus on the use of encryption to protect content in the face of persecution, targeting, and government surveillance due to this group’s activities and views. However, this has not always been the case. Following the public disclosure of U.S. government documents by Edward Snowden in 2013, many in the independent voices community became aware of the need to encrypt data and communications in the face of modern surveillance techniques.\textsuperscript{51} Shortly thereafter, secure messaging applications incorporated end-to-end encryption by default, making the technology easily accessible and requiring little to no training to be effectively used. Individuals must also consider the global landscape of encryption and cybersecurity policy. For users operating across borders or within restrictive environments, restrictions and regulations that vary from country-to-country may impact the use of encrypted messaging, VPNs, and other protections.

While individuals may quickly adapt their security practices, organizations such as newsrooms and NGOs must also adapt their physical and digital security at an enterprise level. Dynamics between individuals and company leadership often impact adoption efforts, as noted by Kate Krauss in a 2017 article for Wired: “Journalists who do use encrypted privacy tools often face an uphill battle from editors and publishers who need convincing that online security is essential.”\textsuperscript{52} As a result, organizational implementation of encryption use often lags behind individual use.

**IMPACT OF ENCRYPTION POLICY ENVIRONMENTS**

For independent voices users, the scale of use in society is a factor in the impact of policy choices. Prior to widespread use, encryption and other technology for protecting digital activity could serve as a “signal flare” for the governments interested in who was trying to hide their messages. Encryption was often met with distrust and the assumption that the user had something to hide. In the past decades, encryption has become a staple of large-scale industries such as e-commerce, health care, and finance as well as person-to-person communication.

Widespread use, however, does not stop governments from seeking to access the content protected by journalists, activists, dissidents, and other users. Further, the spread of sophisticated hacking capabilities to nations without legal protections or strict limits on use has compromised the security of independent voices globally.\textsuperscript{53} The strength of end-to-end encryption means that breaking the encryption itself is a significant challenge. Encryption workarounds may be comprised of technical means or legal justifications. Users often face policies designed to bypass encryption through compromising the device, web browser, or other applications. As mass protest movements depend on online coordination and mobilization, internet shutdowns are becoming one mechanism for stopping coordination and mobilization of movements that depend on internet connectivity.\textsuperscript{54} Internet censorship and access denial, as well as full internet shutdowns, can be used as mechanisms for blocking use of encryption. State actors may infiltrate encrypted communication channels to spread disinformation or impact user behavior, namely by disrupting applications and server connections to drive users to less secure forms of communication or compromised applications. Some governments continue to explore extreme measures to gain access to information. In Syria, for example, independent voices have documented the torture of other journalists and activists by the Assad regime for access to Facebook and device passwords.\textsuperscript{55}
AT-RISK GROUPS

The at-risk user group includes those marginalized by governments and societies based on their identity or minority status, on the grounds of race, gender, ethnicity, sexual orientation, or other forms of identity. At-risk users may also be those who require protection based on circumstance or surroundings, such as victims of domestic abuse or violence, medical personnel in conflict environments, and refugee or migrant populations. At-risk communities share many concerns with the independent voices community in using encryption for privacy and security to minimize risk of persecution or prosecution. However, a distinction for these users is that the risk is not solely from government access to information. Social persecution may come from the general population. The pressure exerted on at-risk communities is not only from law enforcement. Many users actively work with law enforcement to secure their digital footprint. For example, domestic violence victims may work with law enforcement officers for education on technology that does not leave a digital footprint and cannot be tracked. In this case, there is no political animosity toward these users despite the strong need for privacy and protection.

USER APPLICATIONS

Person-to-person Communication:
Encryption allows users to maintain privacy of activities and communications to minimize exposure and risk of violence against at-risk communities. Encrypted messaging services are used to facilitate safe and secure communication within communities. Beyond person-to-person communication, encryption provides a means for at-risk users to communicate securely with organizations. Encryption provides methods of communicating anonymously with health care or other public health entities. Encryption is relevant to protect health care information generally, but it becomes a safety and security concern for users who need access to health care and the ability to share information about health concerns or diseases that could result in marginalization due to social stigma.

Groups and Community Building: Unsecure or open applications used for community building or facilitating connection may be exploited by malicious actors who seek to harm users. Users turn to encryption to protect digital fora for safely building communities and sharing information with other at-risk users. For example, women in India have found safe harbor in encrypted communications as they navigate the risk and aftermath of sexual assault. On the other hand, features on popular encryption apps such as radio and broadcast functions can also be exploited by those seeking to target at-risk populations, including through the spread of propaganda and incitement of violence against them.

PRIORITIES AND CONSIDERATIONS

For many in at-risk communities, encryption is a means to maintain privacy for protection of individuals and communities. In addition to preventing unwanted monitoring, this includes preventing exposure of personal details and the public view of identifiable information that could result in, for example, targeting, stalking, or physical harm. Targeting may
be conducted by individuals who seek to harm others or by governments who seek to broadly persecute marginalized groups. Encryption combined with mechanisms to ensure anonymity are used to protect citizens from crime, threats, and violence.

**IMPACT OF ENCRYPTION POLICY ENVIRONMENTS**

The severity of threat to at-risk groups often varies on a country-to-country basis. As many at-risk communities are localized within regions or countries, policies that limit or restrict broad access to encryption are most impactful. In countries that search for users of encryption services, tools for privacy and anonymity online provide signatures that governments may look for to disrupt service and identify users. Governments that do not seek to restrict certain key features of encryption applications, such as limits on the size of groups and restrictions on radio and broadcast dissemination lists, may also put at-risk communities at even greater risk from digital propaganda, incitement, and direct targeting from groups that seek to marginalize them. Policies that restrict access to easy-to-use default encryption create significant barriers to the average user. Further, individuals are also less likely to have organizational or institutional support in learning techniques to minimize digital footprints.

Many of the concerns surrounding civil liberties and access mandates from the independent voices user community remain relevant. While concerns of state surveillance exist in both authoritarian and democratic societies, access mandates could be particularly problematic in authoritarian countries with few protections for civil liberties. In liberal democracies, a combination of technical security measures and governance and legal protections can provide some protection against misuse of data by governments, though concerns of due process and regulation of appropriate use are active topics in legal proceedings. In authoritarian states with few legal protections and little or no oversight of law enforcement and intelligence agencies, not having access to easy-to-use, widely available, and secure encryption by default could leave users vulnerable.

When content cannot be accessed, metadata analysis presents a challenge for at-risk users. Metadata is not a substitute for access to content of communications or stored data. For example, while metadata could establish that two criminal suspects are communicating frequently, it could not prove beyond a reasonable doubt that they are conspiring to commit a crime. For those in at-risk communities, however, metadata and location data potentially provide sufficient information for malicious actors who seek to target or threaten users. As messaging platforms place content out of reach, metadata may remain unencrypted to preserve revenue streams. Furthermore, in many jurisdictions there are few restrictions on the collection, use, and retention of non-content data, which could lead to intrusive surveillance practices.

**BUSINESSES AND ORGANIZATIONS**

Beyond use by individuals, businesses and organizations need encryption to secure data and communications. In the Information Age, digital security is an essential part of running a business. Data breaches that expose significant amounts of consumer and sensitive data routinely make head-
Encryption intersects business interests in a number of ways. Organizations must contend with the threat of cybercrime and cyberattacks, law enforcement data requests, and the implications of requirements on data localization and data privacy, to name a few. Encryption is necessary for the security and privacy of customer and employee information. Robust cybersecurity practices, including the use of encryption, are also necessary for the prevention of cybercrime and targeted activity from a range of actors (i.e., state-based threats to individual cyber criminals). Further, businesses must contend with the use of encryption against them, as is the case in ransomware that employs encryption to launch attacks, secure information for ransom, and collect the requisite ransom.

**USER APPLICATIONS**

**Person-to-person Communication:** The protection of person-to-person communication is necessary for internal discussions as well as for the protection of communications between outside individuals (e.g., funders, customers, consumers, and stakeholders) and business employees or representatives. As part of the enterprise information technology functions, businesses manage services that allow employees access to a wide range of accounts for communications. Messaging services used for internal conversations risk exposing intellectual property, trade secrets, or embarrassing information if compromised. Details of business arrangements, contracts, and projects are routinely exchanged via email between businesses and outside stakeholders. For industries such as health care and banking, encryption allows for messaging and communication services that comply with existing privacy regulation (e.g., HIPAA-compliant messaging services in the health care industry) to protect user data and personally identifiable information (PII).

**Information Storage:** Businesses and organizations also use encryption to secure and protect the information they collect. Physical security is enabled through encrypting the data stored on devices or infrastructure such as computers, phones, and servers. As cloud storage services become the norm for many businesses, cloud providers use encryption to secure data in transit, data being moved to the cloud, and data at rest, as well as data stored on the cloud providers’ servers.

**Financial Transactions and Commerce:** The banking and financial industries already employ high levels of encryption to protect consumer and transaction data in both storage and transmission. Encryption is also an important part of securing mobile financial applications that have grown in popularity and use, such as person-to-person payments.

In addition to internal uses and support of operations, companies market encryption to attract users to their product offerings. Businesses find a viable market for security-as-a-service product offerings that incorporate the encryption necessary for privacy, data management, and system security. While chat or messaging services aim to attract individual users, companies also market to other organizations and companies to provide security solutions. Encryption for system security remains relevant for industrial control systems and operational technology, however, the Internet of Things (IoT) and spread of “smart” technologies requires the security of a myriad of devices now be connected to the internet and each other. For these industrial infrastructure applications, encryption becomes a public interest when it ensures critical infrastructure remains secure and available.

**PRIORITIES AND CONSIDERATIONS**

The most pressing considerations for businesses using encryption are privacy and cybersecurity. Social media and messaging apps continue to look to unrecoverable encryption in their product offerings to ensure the privacy of their consumers’ communications and data. Businesses and organi-
izations use recoverable encryption to protect the privacy of their employees, their customers, and other external stakeholders, namely by preventing unwanted monitoring and disclosure by technology companies, governments, and other third parties. Businesses must also comply with privacy regulation and standards that may require the use of encryption. Businesses must safeguard data and devices from cybercrime, hacking, sabotage, and espionage. They must consider the digital security of their internal infrastructure as well as product offerings. While businesses have incorporated some level of cybersecurity in their operations for years, the steady pace of large-scale breaches through products and services left unsecure and vulnerable has pushed customers to increasingly prioritize cybersecurity when considering options.

As demonstrated through the cascading effects of state-based cyberattacks such as NotPetya and WannaCry, the digital footprint and infrastructure of organizations means that national security is a growing consideration for businesses. Particularly as critical infrastructure becomes more connected and digital, the confluence of national security and business interests will likely be a continuing trend. Encryption may also be important to protect the integrity of data flowing to and from machines in critical infrastructure businesses.

**IMPACT OF ENCRYPTION POLICY ENVIRONMENTS**

For businesses, there are existing legal and regulatory recoverable encryption requirements for consideration when characterizing the policy environment. Businesses have regulatory responsibilities to protect entrusted customer information. Standards-setting bodies provide guidelines for information protection, as seen in the credit and debit Payment Card Industry Security Standards Council. While the health care, pharmaceutical, banking, and financial industries have needed to safeguard consumer information for decades, most industries must now consider consumer privacy concerns as products and services that are digital or connected to the internet. Given the rise of digital threats, many start-ups and small businesses are hiring security teams early in the fundraising process. However, policy requirements on cybersecurity, data protection, and encryption must consider the potential disadvantage to small companies that may be financially burdened by requirements for large security teams.

On the unrecoverable encryption front, companies that do business in countries with access mandates will also face growing scrutiny from a variety of stakeholders, from consumers to governments without access mandates. At the time of publication, in many countries, including the United States and Brazil, companies cannot be compelled to use only recoverable encryption. However, if companies do have access to users’ communications, they can be required to turn the data over, pursuant to lawful process. Governments are already skeptical of companies’ claims about their ability to access user data when using unrecoverable encryption. For example, Facebook executives have been jailed in Brazil for failing to turn WhatsApp chats over to law enforcement despite statements that communications are protected by unrecoverable encryption. Lawmakers continue to pressure companies to provide technical mechanisms to gain access to information protected via unrecoverable encryption, as seen with proposed legislation in the United States. Companies operating in countries with access mandates may face a choice between significantly altering the security or architecture of products, hacking or compromising their product if legally compelled, maintaining product integrity and operating in open violation of law, or leaving a market entirely. If companies implement access mechanisms to comply with access mandates in some countries, others will expect the same access to user data, even if they do not have their own access mandates.
While concerned with the challenges encryption can pose to public safety, national security and foreign policy officials in the United States and like-minded nations are themselves turning to commercial encryption platforms for informal—and sometimes formal—communications and data security.

For diplomats and military and intelligence officers, messaging apps such as Signal, WhatsApp, and Wickr provide a reasonably secure and instant means of communication with government colleagues, local contacts, and foreign officials. End-to-end encryption offers foreign policy officials a means to communicate directly and quickly with foreign counterparts and each other when away from government facilities and systems. Secure instant messaging can help expedite the slow churn of diplomacy, enabling diplomats to receive more rapid responses from foreign officials to routine requests without the typical cycle of meetings and follow-ups. For diplomats, private person-to-person communication is particularly important when engaging sensitive contacts such as political opposition and human rights activists in non-democratic countries. Communicating with Western officials and the content of those conversations could put these contacts at risk. For military and intelligence officers, encrypted messaging apps, particularly those with anonymized and auto-deleting settings, are similarly useful in protecting content and communications with sensitive sources from hostile intelligence surveillance.

Coordination: Commercial platforms are being used to plan, coordinate, and execute diplomacy and military operations across internal and foreign stakeholders. At multinational bodies such as the United Nations, group chats serve as a virtual private forum where diplomats build negotiating positions and consensus and can coordinate in real time with counterparts outside the meeting. Commercial apps are uniquely suited for diplomacy and negotiations with non-state actors such as the Taliban who lack official secure means of communication. For military and intelligence officers, messaging apps enable coordination with foreign partners, particularly on time-sensitive operational issues and when outside secure facilities. In some cases, commercial platforms may be the primary means of communication, such as with non-state actors or partners deemed too high a counterintelligence risk to share or provide communication systems. On the battlefield, messaging apps can even serve as a command-and-control tool in multi-partner operating environments where tactical decisions are urgent and official communications may be disrupted or unavailable. For example, Iraqi security forces reportedly employed WhatsApp group chats to help coordinate ground operations and call in U.S. airstrikes during the fight against the Islamic State in Mosul, Iraq.

Content Sharing: Encrypted commercial apps are also employed for another core mission of foreign policy professionals: field reporting and unclassified “intelligence” sharing. In lieu of the
traditional embassy cable, diplomats may turn to messenger apps and group chats to deliver time-sensitive reports and receive guidance from their capitals. During times of instability and crisis, these platforms are also useful in collecting and vetting information from the ground and host-nation government and communicating guidance to citizens in country.83

**PRIORITIES AND CONSIDERATIONS**

For the United States and like-minded foreign policy communities, encrypted communications can help facilitate their top priority: promoting national security and their country’s interests abroad. Whether negotiating diplomatic initiatives, conducting military operations with local actors, or contacting intelligence sources, encryption provides an important tool for the day-to-day communication and coordination needed to execute foreign policy and security missions. In considering the use of encryption, foreign policy officials often have two other key priorities: cybersecurity and privacy.

When operating in the foreign field, encryption assists diplomats and military and intelligence officers in securing data and communications from routine foreign intelligence collection and hostile surveillance from state and non-state actors.84 Moreover, the threatened integrity of unclassified government systems and aggressive “hack-and-release” efforts from state and state-sponsored organizations such as WikiLeaks that target classified systems have heightened cybersecurity concerns. Officials may opt for commercial apps with strong encryption and auto-deleting in some operating environments, particularly for sensitive correspondence.85

Along with cybersecurity concerns over espionage and hacking, foreign policy officials may also opt to communicate and disseminate field reports via commercial messaging apps for a different reason: risks to secrecy and privacy, not from foreign surveillance but from internal leaks. In an era of increasingly divisive politics in Western democracies, diplomats who perceive a lack of political cover for candid field reports and fear their assessments may be leaked for perceived domestic political advantage may favor messaging apps and private group chats to convey sensitive information and limit distribution of content.86

**IMPACT OF ENCRYPTION POLICY ENvironments**

For national security and foreign policy officers abroad, the use of encryption depends as much on the status and nature of the diplomatic and intelligence relationship between their home and host countries as it does on the specific encryption policy regime and technical capabilities of the host-nation government. Countries with design mandates that facilitate access to encrypted data, such as China and Russia, are also countries that aggressively and consistently attempt to monitor and decrypt communications of foreign officials, particularly the United States. In such a high counterintelligence risk environment, foreign officials likely assume all commercial encryption is compromised and thus of little utility. In countries where any access to commercially encrypted communications is prohibited, diplomats and military and intelligence officers will be free to employ tools furnished by their home country with limited ability for host-nation monitoring.

Rather, encryption policy choices are most impactful to foreign policy professionals in countries with some type of decryption mandate and that reside diplomatically somewhere between adversary and ally. For nations with technology-neutral or user decryption mandates, diplomatic, military, and intelligence uses of commercial apps will likely depend on how aggressively and consistently host-nation services attempt to monitor and decrypt their communications as well as on any official protocol or informal understandings among governments on surveillance. Nations risk diplomatic fallout if attempts to demand access to decrypted communications from technology firms and service providers are discovered, while compelling foreign officials to disclose private encryption keys is even less likely, barring some substantial diplomatic breach.
Perhaps most acute for foreign policy professionals are countries opting for encryption access workarounds, specifically lawful hacking or “ghost key” capabilities. Even relatively friendly countries may be tempted to employ such capabilities for intelligence collection purposes if confident their access can remain clandestine. More concerning are neutral or quasi-adversarial nations who can develop or commercially procure high-end hacking and decryption capabilities, obtain such technology from China and Russia, or permit foreign actors to conduct their own collection and hacking efforts in country. Indeed, with persistent and often effectual efforts from cyber powers to break commercial encryption combined with hacking to compromise personal devices and gain access to data, commercial apps will likely remain only a secondary choice for foreign policy professionals with critical and sensitive communications.

**USER APPLICATIONS**

**Broadcasting and Information Dissemination:** While private, one-to-one communication remains a key use of encryption, terrorists and extremists are increasingly exploiting the broadcasting features of encrypted messaging apps to disseminate propaganda as well as identify like-minded adherents and potential recruits. Islamic State leadership in Syria and Iraq has leveraged public and invite-only channels to test, develop, and disseminate core themes and messages before coordinating with global affiliates to tailor the propaganda to local audiences. White nationalist and neo-Nazi extremists are similarly exploiting the fluidity of “dual-use” apps to move between public broadcasting of “news” and propaganda to private channels for targeted messaging and more direct advocacy of violence. Telegram, in particular, has become an integral propaganda tool of the far right, with more than 100 channels promoting “white accelerationism” and “terrorwaves” of attacks targeting minority communities.

**Person-to-person Communication:** After using public channels to “find” like-minded supporters, terrorist and extremist groups can then “filter” potential recruits into private group chats and “funnel” the best prospects to more direct and secure encrypted communication. The Islamic State, Al-Qaeda, and Hezbollah have leveraged this technique in particular for recruiting members inside Western or other “enemy” countries, identifying engaged users in app channels and social media, contacting them via direct message, and then...
moving the conversation to secure chat or encrypted email. Once in private and encrypted channels, new recruits then receive sensitive instructions for a specific course of action and tips for enhancing operational security, such as the use of VPNs, anonymization, and location data hiding tools. Similarly, neo-Nazi extremist groups such as the American Atomwaffen Division and Western affiliates such as FeuerKrieg Division use Telegram’s public channels and social networking sites such as Gab as advertising tools, encouraging potential new members to contact them securely via ProtonMail addresses posted on these platforms.

Groups and Community Building; Content Sharing: As military and security forces degrade physical safe havens, encrypted private channels and group chats have become terrorists’ virtual safe havens, where they can build and expand their extremist communities and inspire and radicalize members with steady streams of propaganda and content. For the far right, private channels and groups enable extremists to build bridges to like-minded communities and individuals across the globe, hone themes and standards for internal and external messaging, and share sensitive content such as targeting techniques and weapons production guides for attacks. For jihadists, group chats often serve as a “public square” to air grievances and perceived injustices perpetrated by local and foreign governments to radicalize members, while smaller groups are used to build tighter communities inside “enemy” countries to deepen bonds and enhance security. While far-right extremists and Salafi-jihadists alike probably believe their channels and chats are being monitored, both have concluded the value offered by community building and content sharing commercial apps outweighs the potential risks.

Coordination and Mobilization: After spotting supporters on social media, recruiting them via encrypted messaging or email, and radicalizing them further in group chats, extremists then seek to “operationalize” these tools to coordinate and execute attacks. The Islamic State’s Syria-based external operations wing exploited encrypted instant messaging apps to direct dozens of attacks in Europe and other Western nations from 2014 to 2017. During the Paris attacks in November 2015, Islamic State members used Telegram direct messaging and group chats to coordinate throughout the multi-pronged attack, later employing the message self-destruct feature to disrupt future law enforcement investigations. Hezbollah, too, has attempted to use encrypted messaging to direct plots inside “hard target” foreign countries such as Israel and the Palestinian territories. Commercial encryption provides perhaps even more favorable terrain for the far right, as countries vary dramatically in their level of monitoring of white nationalists and neo-Nazis as compared to jihadist groups.

Commerce and Financial Transactions: While informal money transfer systems such as hawalas and traditional bulk cash transfers remain the primary means of terrorist financing, encrypted peer-to-peer (P2P) payment systems and even cryptocurrencies are now being exploited to fundraise, move money, and purchase materiel for attacks. As “digital wallets” and P2P money transfer tools such as PayPal, Square, and Venmo become more accessible and secure, groups ranging from the Islamic State to Hamas to white nationalists have used them on occasion to transfer funds to foreign cells and “lone wolves” to facilitate attacks. The growth of P2P platforms and increasing ease of use suggest greater attempts at adoption by terrorists and extremists in the short term. While P2P firms have bolstered cooperation with governments and “know your customer” regulations, their enhancement of encryption and anonymity features will make detecting terrorist use more difficult.

Priorities and Considerations
For terrorists and extremists, privacy in communications and security of data in transit and at rest are the top priorities when considering the use of
encryption. However, adoption of encryption tools for recruitment, radicalization, and attack planning requires some important trade-offs.

From a privacy perspective, terrorist and extremist groups must balance the need for secrecy and anonymity in sensitive communications necessary to coordinate attacks with the need to publicize their cause, engage potential recruits, and expand their global reach. The need to balance these private and public efforts is one reason “dual-use” apps with public channels and private encrypted messaging have become so vital to terrorists and extremists.\(^\text{105}\) Extremist groups—particularly those on the far right—tend to opt for commercial platforms from firms that minimize private data sharing with governments, such as Telegram. Far-right extremists also tend to use coded language in public or semi-private channels that stops short of directly advocating violence to avoid attracting or complicating government scrutiny.\(^\text{106}\)

From a cybersecurity perspective, terrorists and extremists have historically faced a trade-off between functional ease of use on commercial platforms and their level of security against espionage and hacking. Until recent years, terrorist groups such as the Islamic State often used relatively insecure means of communication such as text messages due to their simplicity and widespread use among members.\(^\text{107}\) However, as end-to-end encryption became the default setting on several popular messaging apps, this functionality versus security trade-off has largely vanished because automatic encryption of messages and calls has enhanced terrorist and extremists’ “operational security” without any change in their practices and technology use.\(^\text{108}\)

**Impact of Encryption Policy Environments**

Countering terrorist use of encryption technology, particularly jihadist groups such as Al Qaeda and the Islamic State, is among the few areas of agreement among world powers on global encryption policies, creating challenges for terrorists and extremists across most operating environments. Yet their ability to operate in the digital terrain will vary across the mandated access spectrum. Nations with favorable access regimes, high-end decryption, and intelligence capabilities, or access to similarly capable commercial hacking tools (primarily authoritarian states), will be inhospitable for terrorist communication. But in democracies, terrorists’ ability to exploit encryption will vary with differing decryption mandates and rule of law for surveillance.

In countries with technology-neutral mandates, terrorists will be hard-pressed to maintain private encrypted communications, but the level of risk depends on how rigorously governments enforce mandates and how willing technology companies are to cooperate. For issues such as terrorism, and when facing heavy penalties such as fines and imprisonment, commercial firms are more likely to comply and provide decrypted data upon request to the government. In this operating environment, extremists will likely seek to optimize anonymity and auto-delete features on commercial platforms to minimize risk of exposure and data loss.

For countries with user decryption mandates, extremists’ first line of defense will be to avoid being detected and arrested, but if they are, it will be critical to have their device security maximized to prevent access. Savvy and well-trained terrorists—not the majority—may opt not to disclose encryption keys to law enforcement to avoid the potentially greater consequences from what is found in their decrypted data. They may likewise avoid use of biometric keys that can be involuntarily applied and utilize auto-deleting features. Terrorists operating in countries with decryption mandates may also benefit from using platforms such as Telegram where decryption keys are spread across multiple data centers worldwide, requiring local law enforcement to gain approval from multiple governments and resulting in slower or even denial of access.\(^\text{109}\)

For countries with lawful hacking mandates, terrorists’ ability to utilize encryption for secure
communications will depend almost entirely on the hacking and decryption capabilities of domestic intelligence and law enforcement. For nations where the government has no legal way to access encrypted communications, data, and devices, terrorists and extremists will have freest use of the digital terrain, though still facing the traditional tools and tradecraft of law enforcement.

If past is precedent, terrorists and extremists will adapt to evolving government approaches to digital monitoring and encryption, moving from insecure or compromised platforms to new ones in a perpetual race to stay ahead of intelligence and law enforcement. However, their ability to do so depends not only on specific encryption laws and policies but also on the political will of governments to apply and enforce them, which in turn can depend on the nature of the group. In particular, far-right extremists and white supremacists in the United States and other Western democracies are protected by free speech and exploit these legal protections in their use of encryption by using coded language or stopping just short of explicitly advocating violence, enabling them to evade monitoring and avoid arrest.
Encryption presents a multifaceted challenge with significant consequences. The future of encrypted applications is playing out on a global stage across various regional and national scenes. All kinds of people and communities use encryption, from those most deserving of society’s protection to those from whom society must be protected.

Given this dynamic, there is no single takeaway or algorithmic framework that clarifies its complex nature for policymakers. The global encryption policy landscape will continue to evolve in coming years as governments struggle with the “Going Dark” challenge. Different countries will pursue divergent approaches, some restricting the availability of unrecoverable encryption and others accepting the free availability of encryption while pursuing alternative investigative and intelligence tools. Developed Western nations such as the United States, Australia, and the United Kingdom face challenging cases that could define the boundaries of their encryption laws. Developing nations such as Brazil and India continually struggle to balance
developmental goals and security with technology adoption in their populations. Amid these national-level changes, providers of encrypted products and services will continue to advance the technology and adapt their approaches.

These realities only serve to underscore the critical role good encryption policy and oversight play in ensuring citizens’ rights and safety are secured within a democracy. The findings of this study should inform lawmakers and the legal community in the United States regarding users and the policy environments in which they should operate.

**Summary User Findings**

Policy changes will have different impacts on stakeholders around the world. For some, changes in lawful access policies will have little impact. For example, most email uses recoverable encryption, as do most corporate networks, meaning they will be unaffected by most encryption policy regimes. Encryption policies also do not exist in a vacuum. For users in liberal democracies, strong governance and accountability mechanisms, independent legal systems, and clear principles and use cases guiding access mandates provide protections against intrusive surveillance practices, even if access to unrecoverable encryption is limited. There are technical measures other than encryption that might be used for secure storage and communication, whether ephemeral services, air-gapped networks, or simply going back to analog tools. Some, both malicious actors and at-risk populations, will leverage free and open-source technology to encrypt their own data and devices.

**Encrypted communications are becoming ubiquitous.**

Across all user groups examined in this study, encrypted communications are on the rise. This outcome is unsurprising, given the overall increase in availability and use of encryption. Moreover, encryption aids digital security and physical security, which all actors—from benign to malign—seek. It is notable that while all user groups examined in this study rely on encryption for person-to-person communications, none limit its use to that single purpose. Evidence suggests that every user group is turning to encryption for at least three applications, prioritized in accordance with their needs.

For example, in considering approaches to addressing growing encryption use, law enforcement and public safety users—e.g., local and federal law enforcement agencies and officers, first responders, lawyers, and judges—must recognize that policy choices would also impact their access to and quality of secure technology. As with all other users of encryption, public safety users benefit from accessible and easy to use encryption solutions, mobile device security, and encryption to secure data transmissions. Public safety users may find themselves targeted or have personal details made public. Unencrypted communications by public safety users may also reveal personal details about civilians, including those at risk and minors. However, the use of encryption by public safety users is not without its concerns. The use of encrypted radios by police officers raises questions about transparency, accountability, and oversight.

**Uses of encryption vary within and across user types.**

Users may find themselves at the nexus of framework communities and may also use encryption in everyday activities. Users continually balance maximizing security and best practices with the effort level, comfort level, or accessibility of encrypted platforms, digital hygiene practices, and cybersecurity. The primary considerations for choosing a particular encryption application also appear to vary within and across the groups. For some, such as a nascent dissident group, an application’s ease of use can be a determining factor in choosing it. For others, such as seasoned journalists and security professionals, security features like end-to-end encryption matter more than usability. The CSIS study team anticipates these
distinctions will narrow as both encryption technology and user interfaces improve.

In some environments, users will also be considering the chance that the mere act of encrypting data or communications could draw unwanted attention from a government, company, or other monitor. In more repressive regimes, for instance, a citizen tempted to rely on open encryption tools to protect oneself from government surveillance may not do so if they believe it would serve to flag their existence or activities.

**Encryption policies will need to account for “good” and “bad” users.**

This study’s analysis of specific user groups serves to highlight that, for free peoples and their governments, the implications of ubiquitous encryption use do not cut only one way. The same encryption that protects the safety and security of a journalist, dissident leader, or diplomat can create opportunity for violent extremists, criminals, or corrupt officials to undermine public welfare. Further, as the governance environment changes, so too do the user group considerations around encryption. For instance, during the Arab Spring, encryption allowed groups to communicate and organize peacefully in support of improved representation and governance. However, as crackdowns occurred, encryption became a tool that governments used to identify and persecute those same dissidents.

**Users continually assess risks and adapt practices accordingly.**

Each of the user groups in this study arrives at a decision to use encryption based on an assessment of the risks they face. Whether the result of a formal systematic evaluation or more informal trial-and-error adoption of best practices, user groups perform a trade-off analysis to adapt their cybersecurity posture based on their understandings of the threat environment, identify the best opportunities to reduce risks, and balance the effort required to protect their data and digital footprint. For example, journalists and intelligence professionals may take aggressive measures to reduce their digital footprint (in addition to communicating via encrypted channels) that may have too high a bar for adoption for many users, such as eliminating credit card usage and social media presence, storing electronics in faraday cages, discontinuing use of applications that store personal data, and adapting communication practices with the assumption that devices are compromised. Their security practices are based on a threat matrix and risk assessment that include targeting by sophisticated foreign adversaries where the consequences of exposure outweigh the inconvenience of their security posture.

**Summary Policy Environment Findings**

As more countries look for solutions to the “Going Dark” challenge, there will be significant implications for encryption users around the world. Encryption policies that restrict access to unrecoverable encryption increase access to data for law enforcement and security agencies but could also create vulnerabilities that could expose private communications and sensitive data to malicious actors. While lawful hacking does not require exposure of these private communications, it could undermine systemic security by limiting government disclosure of vulnerabilities to hacking.

**Completely preventing use of encryption is impossible.**

Governments globally are using a variety of tactics to prevent access to information and communications: internet shutdowns, blocking mobile phone access, and blocking messaging application services. Indeed, in the face of unsatisfactory technical solutions to content access, countries may pursue outright bans on the use of encryption and limited access to the internet, as seen in Russia’s attempt to ban Telegram by blocking access through internet service.
providers and requesting the application’s removal from Google and Apple application stores.\textsuperscript{320}

Even the most restrictive policy regimes cannot completely cut off access to unrecoverable encryption or prevent actors from using encryption to hide their activities.\textsuperscript{321} Encryption is applied mathematics, and a sufficiently skilled and educated user can develop their own encryption systems based on widely available mathematical principles. Open-source code for encrypted communication, for example, Pretty Good Privacy (PGP), is freely available online. However, creating truly unrecoverable encryption is extremely difficult, and even major technology companies with large talent and resource pools struggle to implement it correctly and securely.

**National policy regimes have global implications.**

While countries are pursuing a range of policy options related to encryption, the implications of those policy decisions can extend beyond their own borders for the business community and multinational organizations. One of the central themes in the global encryption policy space is the degree to which variation in understanding and recognition of a right to privacy impacts policy choices. Regional encryption policies that arrive at decisions on the value of private space for communication will impact users who act globally or across borders. If design or technology-neutral mandates become prevalent, global companies could be forced to change the way they build and operate their products, thereby impacting their users in countries without restrictions on encryption.

Companies prefer to build one international product that they can operate across global markets instead of selling different products in different markets. While some nations may be willing to negotiate with corporate entities, nations taking a hard line on design or technology-neutral mandates would force companies to choose between market access and changing a product offering. If enough markets implement access mandates that make unrecoverable encryption illegal, multinational companies might be forced to adopt recoverable encryption for their global products. When mandates impact the use of encryption for internal processes, businesses may also be forced to consider the value and viability of their physical presence in a country.

**How companies react matters.**

As countries change their policies around encryption, companies that provide encrypted products and services will be forced to adapt to this increasingly complex environment. In some cases, companies that offer unrecoverable encryption products or services may choose to exit markets that require access to encrypted data. In other cases, companies may choose to create a custom version of their product for that market that utilizes recoverable encryption but continue to use unrecoverable encryption outside of that country. Finally, some companies may be forced to utilize recoverable encryption for all of their users if a large enough share of their market mandates recoverability.

But forcing companies to maintain the capability to decrypt their users’ data for governments will not necessarily ensure government access to that data. Already, companies are pursuing means other than encryption to shield their data from intrusive governments or malicious actors. A growing number of services offer “ephemerality,” meaning they delete data instead of storing it to ensure that it cannot be collected, lawfully or unlawfully. Others store their data in overseas markets where it is outside of the jurisdiction of local authorities or use a technique called “sharding” in which they store parts, or “shards,” of files across multiple data centers, making it more difficult to access illicitly.

**Vulnerabilities in encryption systems are prime targets.**

Authoritarian governments are not the only ones that could exploit lawful access mechanisms. While
policymakers are focused on ensuring access to encrypted data for law enforcement and security agencies, limiting access to encryption will have broader implications. Access mechanisms designed to allow companies to reach user data could be targeted by criminals or foreign intelligence agencies. If a malicious actor succeeded in compromising a vendor’s encryption keys or identified a vulnerability in a prescribed encryption algorithm, it could allow them to easily exploit user data at scale.

Encrypted communications are only as strong as the encryption used to protect them. Many commonly used encryption protocols available today purport to be unbreakable, featuring keys so long that it would take even a supercomputer trillions of years to guess. However, flaws in the way a protocol is implemented can provide malicious actors with the opportunity to quickly break the encryption in a much shorter period. In 2017, for example, researchers discovered a flaw in a code library used to secure more than 750,000 Estonian e-ID cards that would allow attackers to calculate some keys in as little as 45 minutes. This attack targeted the RSA encryption protocol, one of the most popular in the world, and one which was imbedded in an implementation that had undergone rigorous examination, including compliance with two international security certification standards. Many such instances of attacks on poorly-implemented encryption schemes have been documented, and these pose a continuous threat to the security of encrypted systems.

Encryption can also be broken by gaining access to the keys used to decrypt digital content. Recoverable encryption systems are particularly vulnerable to these forms of attack, as encryption providers deciding to maintain some form of third-party access will be forced to maintain repositories of users’ keys, a prime target for malicious actors. If hackers can successfully gain access to these key repositories, they will have the ability to decrypt all of the communications of that company’s users. Security professionals rate key management as one of the most challenging aspects of cybersecurity due to the difficulty of adequately securing encryption keys and the potential damage of a breach. One notable example of an attack on a key repository was an operation by the National Security Agency (NSA) and GCHQ to steal the encryption keys used to secure the SIM cards of mobile phones. Such an attack would easily allow the key holders to bypass encryption by directly accessing the content of users’ phones. Encryption can also be broken by targeting end devices with forms of malware that access communications content before it has been encrypted, as in the case of a recent WhatsApp vulnerability that allowed spyware to be installed by calling the target’s phone.

Alternatives to access mandates bring their own challenges.

Without the ability to access encrypted data through service providers, law enforcement and security agencies are unlikely to merely accept that significant amounts of data are out of reach. Some experts who oppose restrictions on encryption point to lawful hacking and metadata analysis as alternative investigative techniques, arguing that more data on our preferences, thoughts, and behavior is available than ever before. Countries that do not implement restrictions on encryption are likely to pursue alternative means of accessing encrypted data and expand their abilities to mine unencrypted data such as metadata and data from IoT devices. Even countries that do pursue restrictions on encryption are expanding their hacking and data analytics capabilities.

Lawful hacking regimes are often described as less of a threat to the cybersecurity and civil liberties of users when compared to access mandates, but they also bear significant risks and challenges. On one hand, not requiring lawful access mechanisms removes the potential risk of introducing cybersecurity vulnerabilities into a system when building in new access mechanisms. But the challenges of acquiring, maintaining, and using lawful hacking ca-
pabilities also make it difficult to use these authorities to conduct surveillance quickly and at scale.

Ensuring that robust controls and appropriate accountability mechanisms are in place is essential. In Germany’s case, their legal framework places strict limits on when and how lawful hacking can occur. Police may only conduct hacking operations when there is a specific impending danger to lives or the state. Requirements for judicial approval are used to ensure oversight over the process, and restrictions on accessing “core” information, such as family communications or communications between the target and their doctors or attorneys, create additional safeguards for civil liberties.128

**Overreliance on lawful hacking puts security at risk.**

Lawful hacking requires a degree of secrecy and opacity that creates challenges for oversight, accountability, and due process. Hacking a device could also result in the incidental collection of significant amounts of sensitive data that have nothing to do with a legitimate investigation or intelligence operation. For example, hacking a smartphone to gain access to one criminal conversation could expose everything from personal photos to private documents to notes and communications with friends and family.

Backdoors into platforms and devices would create vulnerabilities in the same devices that public safety users use in both their personal and professional capacities.129 Balancing equities is all the more challenging when governments depend on lawful hacking for domestic data access. The “vulnerabilities equities process” (VEP) used in the United States to decide when to disclose versus retain vulnerabilities discovered by U.S. government agencies, for example, has had a heavy bias toward disclosing vulnerabilities that affect U.S. citizens and companies and could be used against U.S. targets but has been more likely to retain vulnerabilities and exploits that primarily affect foreign users or that are useful for foreign intelligence collection. If government agencies are dependent on lawful hacking for domestic data access, they will be forced to retain more vulnerabilities for lawful hacking, potentially increasing cyber risks to U.S. networks.

Lawful hacking regimes also raise the question of how to balance the need to maintain a set of hacking tools with the goal of promoting cybersecurity for citizens. Vulnerabilities that governments develop for lawful hacking are not disclosed to vendors to patch, raising the risk that malicious actors will exploit those same vulnerabilities. In some cases, these capabilities may end up leaking to the public and becoming available to a wide range of criminals and espionage agencies that could exploit those vulnerabilities against public safety users.

**Data and technology policies will have second-order effects on encryption policy and user priorities.**

While data policies such as the European Union’s General Data Protection Regulation (GDPR) may not regulate or require the use of encryption per se, encryption is one mechanism by which companies will seek to comply with policies on data protection, privacy regulations, and security requirements. With the global encryption policy already uneven, data localization efforts and the trending assertion of national borders in the internet provide additional fissures across which individuals and businesses must navigate.130 Design mandates on devices and applications, though not explicitly addressing encryption, may also impact the availability and use of encryption. For example, a law passed in 2019 in which Russia required that devices such as phones, computers, and smart TVs manufactured by foreign companies be sold in country with Russian applications pre-loaded was criticized within the industry.131 One point of contention, in addition to threats of surveillance and spying on users, was that the move may result in companies leaving the market if compliance proved too difficult.
Coordination, training, and resources are necessary to support law enforcement efforts in the digital era.

Law enforcement and legal efforts must continually reconcile the need to provide evidence (often message content) beyond a reasonable doubt with protection of free speech, the ease of access and ubiquity of encryption, and the lengthy timelines for legal cases to work through the court system. For example, the complaint brought against several white nationalist organizations following the August 2017 “Unite the Right” rally in Charlottesville, Virginia, cited various communications from Facebook, Twitter, YouTube, and other social media websites. The concern exists that as more of these communications move out of reach to secure channels, efforts to disrupt and prosecute these malicious actors will be significantly hindered. Certainly, this debate over lawful access, both legal and technical, will play out in years to come. In the meantime, messaging platforms continue to incorporate security features, sometimes even decreasing the amount of user data stored. Providing resources and training to law enforcement agencies, as well as increasing coordination across divisions and agencies, can ensure that law enforcement officers and investigators understand what information can be lawfully obtained from communication companies and how to work with such companies. For example, service providers and companies may store unencrypted user data or data secured with recoverable encryption that would be accessible if legally required.
Encryption policy debates are about more than securing data. Authoritarianism is on the rise around the world. In encryption policy, this is manifesting as design mandates from autocrats that prioritize the absolute security of the state over the privacy afforded to individuals, creating real threats to individuals’ safety from the state. The outcome is already visible in places such as Russia and China, where encrypted data is severely compromised, with corresponding risks to companies’ intellectual property and dissidents’ safety.

At first blush, the absence of U.S. encryption policies may seem ideal. Individual freedoms would seem to be maximized, with encrypted communications treated as private space. On deeper examination, however, the case is not clear, as that space may be used to incite violence or systematic repression that threatens the liberty of fellow citizens or the vitality of the democracy itself. Ambiguity on the legal front leaves challenges unaddressed and places undue expectations on the technology.
itself to resolve questions of lawful access. Outright denial of access to encryption and state control of encrypted data and key management is not a viable alternative, however. It errs far more substantially in the opposing direction by eliminating any private sphere free of the government’s view, an intolerable outcome for a free society.

As in other areas of technology policy, there are more alternatives to this dark outcome than doing nothing. This study demonstrates that decisions surrounding when, where, how, and by whom encryption is used can be more nuanced. For instance, if a company implements end-to-end encryption, it may not be able to read the contents of a message, but it might have the ability to monitor certain patterns through metadata that help expose malign actors. Doing this might impede privacy slightly while potentially improving security significantly. There are ultimately several factors that a company or government might consider in determining what is appropriate. The findings of this study can help U.S. policymakers more deftly balance privacy, security, and safety than either extreme on the continuum provides by informing the cost/benefit analysis inherent in any encryption policy choice, including the failure to choose.
About the Authors

Lindsey R. Sheppard is a fellow with the International Security Program at the Center for Strategic and International Studies (CSIS), where she focuses on the role and application of emerging technologies to national security, defense, and intelligence. Her research areas include artificial intelligence, machine learning, defense innovation, and technology ecosystems. She contributes expertise in modeling and simulation, system architecture and design, electronic warfare, and radar from prior experience in defense technology research and development. Before joining CSIS, Ms. Sheppard was a member of the technical staff at the Charles Stark Draper Laboratory and the Georgia Tech Research Institute. During this time, she served as the systems engineering lead on multiyear efforts building simulation capabilities to evaluate technology and deployment solutions to support military operations. She holds an MS and a BS in aerospace engineering from the Georgia Institute of Technology.

Brian Katz is a fellow in the International Security Program at the Center for Strategic and International Studies (CSIS). His research agenda focuses on the intersection of intelligence, national security, and technology and the role of intelligence in policymaking, strategy, and military operations. He also frequently writes on Middle East security issues, counterterrorism, and proxy warfare. Mr. Katz was a visiting fellow at CSIS from 2018-2019 through the Council on Foreign Relations International Affairs Fellowship program. He joined CSIS after a decade of service in the U.S. Government at the Central Intelligence Agency (CIA) and Department of Defense. At the CIA, Mr. Katz served as a military analyst for the Middle East, South Asia, and Eastern Europe, including multiple overseas tours. From 2016 to 2017, he served as country director for Syria in the Office of the Secretary of Defense, where he provided policy and strategy advice on the Syrian conflict and U.S. counterterrorism efforts. Mr. Katz is also an officer in the U.S. Navy Reserve. He holds a BS in economics from Duke University and an MA in international relations from the Johns Hopkins University School of Advanced International Studies.

Dr. Kathleen H. Hicks is senior vice president, Henry A. Kissinger Chair, and director of the International Security Program at the Center for Strategic and International Studies. She leads a bipartisan team of over fifty resident staff and an extensive network of non-resident affiliates dedicated to shaping U.S. national security by providing independent strategic insights and policy solutions. Dr. Hicks has an extensive national security background, including as a senior career executive and a Senate-confirmed leader on policy matters in the Pentagon as well as appointments to two congressionally mandated national defense commissions. In the past several years, she has served as a principal investigator for CSIS on a range of studies relating to deterrence, gray zone challenges, and emerging technology governance. She holds a PhD in political science from the Massachusetts Institute of Technology, an MPA from the University of Maryland, and an AB magna cum laude from Mount Holyoke College.

Joseph Federici is an associate director and associate fellow with the International Security Program at the Center for Strategic and International Studies (CSIS), where he works on a variety of projects pertaining to geopolitics, national security, and defense matters. Mr. Federici also assists in coordinating the CSIS Military Fellows program. He holds a JD from Rutgers University School of Law and a BA in history and political science from Rutgers University. Most recently, he graduated, with distinction, from Georgetown University with an MS in foreign service.
Endnotes


9 For each of the five user groups, the study team provides a generalized assessment from the user perspective with respect to encryption use and privacy, security, and safety considerations. The study team recognizes that individuals within user communities may often have differing levels of awareness and technology use. While there is growing awareness of how individual data is collected and used by companies and messaging services, for many users this remains an opaque topic. Some users may be hyper-aware of the risks they face and use encryption and other technologies accordingly. Some users may simply follow general best practices without conducting their own assessment of the products and services they use. Finally, some users may feel they have little to no use for data protection.

10 Law enforcement and security agencies also face significant challenges in accessing unencrypted data from service providers, as detailed in: Carter, Daskal, and Crumpler, Low Hanging Fruit.


12 Ibid.


18 Kuehn and McConnell, Encryption Policy in Democratic Regimes.

19 National Academy of Sciences, Decrypting the Encryption Debate.


22 Kuehn and McConnell, Encryption Policy in Democratic Regimes.


24 Kuehn and McConnell, Encryption Policy in Democratic Regimes.


29 Standing Committee, The National People’s Congress of the PRC, Cryptography Law of the PRC, 14th Meeting of 13th Congress (Beijing: China People’s Congress, October 26, 2019), http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml.


32 Chris Burt, “U.S. Judge Allows Law Enforcement to Compel Suspect to Unlock Smartphone with Biomet-


39 Ibid.


76 Interview with former U.S. intelligence official, April 2020.


80 Interview with former U.S. intelligence official, April 2020.

81 Gibbons-Neff and Mashal, “In Afghanistan’s War and Peace, WhatsApp Delivers the Message.”


83 Manor, “The Evolution of WhatsApp as a Diplomatic Tool.”
84 Interview with former U.S. intelligence official, April 2020.
85 McTague and Rao, “Leaks are Changing How Diplomats Talk.”
86 Ibid.
88 Interview with former U.S. national security official, May 2020.
95 Makuch and Lamoureux, “After Facebook and Web Host Bans, Far-Right Extremists Are Encrypting and Going IRL.”
96 Interview with Western technology and counter-violent extremism expert, April 2020; and Owen, “How Telegram Became White Nationals’ Go-To Messaging Platform.”
97 Interview with former U.S. national security official, May 2020; and Clifford and Powell, Encrypted Extremism.
98 Interview with former U.S. national security official, May 2020.
99 Clifford and Powell, Encrypted Extremism.
100 Shkolnik and Corbeil, “Hezbollah’s ‘Virtual Entrepreneurs.’”
101 Shkolnik and Corbeil, “Hezbollah’s ‘Virtual Entrepreneurs’.”
102 Hayden, “Far-Right Extremists Are Calling for Terrorism on the Messaging App Telegram”; and Makuch and Lamoureux, “After Facebook and Web Host Bans, Far-Right Extremists Are Encrypting and Going IRL.”

104 Interview with former U.S. national security official, May 2020; and Goldman et al., Terrorist Use of Virtual Currencies.


106 Interview with former U.S. national security official, May 2020; and Makuch and Lamoureux, “After Facebook and Web Host Bans, Far-Right Extremists Are Encrypting and Going IRL.”

107 Interview with Western journalist and terrorism expert, May 2020.


110 Interview with former U.S. national security official, May 2020.

111 Ibid.


113 Encryption Working Group, Moving the Encryption Policy Conversation Forward.


120 Vlad Savov, “Russia’s Telegram Ban is a Big, Convoluted Mess,” The Verge, April 17, 2018, https://www.theverge.com/2018/4/17/17246150/telegram-rus-
sia-ban.


123 Ibid.


133 Signal, for example, by design stores little user information in addition to indicating intent to move beyond use of user phone numbers. Martin Shelton, “Beyond Signal Phone Numbers,” Freedom of the Press Foundation, May 26, 2020, https://freedom.press/training/blog/beyond-signal-phone-numbers/.
