WORKING GROUP PAPER

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

PRINCETON UNIVERSITY

CITP CENTER FOR INFORMATION TECHNOLOGY POLICY

SEPTEMBER 2019

Moving the Encryption Policy Conversation Forward

Encryption Working Group

Moving the Encryption Policy Conversation Forward

Encryption Working Group

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

About the Encryption Working Group

The Carnegie Endowment for International Peace and Princeton University have convened a small group of experts to advance a more constructive dialogue on encryption policy. The working group consists of former government officials, business representatives, privacy and civil rights advocates, law enforcement experts, and computer scientists. Observers from U.S. federal government agencies attended a select number of working group sessions. Since 2018, the working group has met to discuss a number of important issues related to encryption policy, and this paper represents its recommendations to move the encryption policy debate forward.

Members of the Encryption Working Group include:

Jim Baker
Former General Counsel, Federal Bureau of Investigation

Katherine Charlet
Program Director, Technology and International Affairs, Carnegie Endowment for International Peace

Tom Donahue
Former Senior Director for Cyber Operations, National Security Council, White House

Ed Felten
Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University

Avril Haines
Senior Research Scholar at Columbia University's Columbia World Projects and former Deputy Director, Central Intelligence Agency

Susan Hennessey
Executive Editor, Lawfare, and Senior Fellow in Governance Studies, the Brookings Institution

Chris Inglis
Managing Director, Paladin Capital Group, and former Deputy Director, National Security Agency

Sean Joyce
US Cybersecurity and Privacy Leader, PwC, and former Deputy Director, Federal Bureau of Investigation

Susan Landau
Bridge Professor in Cyber Security and Policy, Tufts University

Christy Lopez
Distinguished Visitor from Practice, Georgetown Law Center

Alex Macgillivray
Former Deputy Chief Technology Officer of the United States and former General Counsel, Twitter

Jason Matheny
Founding Director, Georgetown Center for Security and Emerging Technology, and former Director, Intelligence Advanced Research Projects Activity

Tim Maurer
Co-Director and Fellow, Cyber Policy Initiative, Carnegie Endowment for International Peace

Denis McDonough
Visiting Senior Fellow, Technology and International Affairs, Carnegie Endowment for International Peace, and former White House Chief of Staff

Lisa Monaco
Distinguished Senior Fellow, Reiss Center on Law and Security, New York University School of Law, and former Assistant to the President for Homeland Security and Counterterrorism

Laura Moy
Associate Professor of Law, Georgetown University Law Center

Michelle Richardson
Director, Privacy and Data Project, Center for Democracy and Technology

Ronald L. Rivest
Institute Professor, Massachusetts Institute of Technology

Ari Schwartz
Managing Director of Cybersecurity Services, Venable LLP

Harlan Yu
Executive Director, Upturn

Denise Zheng
Senior Associate (Non-resident), Technology Policy Program, Center for Strategic and International Studies

Introduction

The encryption of data and communications has long been understood as essential. Strong encryption thwarts criminals and preserves privacy for myriad beneficiaries, from vulnerable populations to businesses to governments. At the same time, encryption has complicated law enforcement investigations, leading to law enforcement calls for lawful access capabilities to be required of encryption technologies.

The 2016 San Bernardino legal dispute between the Federal Bureau of Investigation (FBI) and Apple over access to an encrypted iPhone provided a snapshot of the contentious debate on law enforcement access to encrypted data. Law enforcement initially argued that mobile device[1] encryption presented a significant barrier to its efforts to investigate a deadly counterterrorism case. Apple responded that the FBI's request that it create software to circumvent its encryption raised unacceptable implications for the security of its broader customer base. The ensuing legal showdown left little room for compromise. The dispute ended when the FBI found a way to access the device without Apple's assistance, so the courts did not resolve the issue.

Since that time, a variety of attempts have been made to move the discussion forward. A report published in February 2018 by the National Academy of Sciences (NAS) enhanced the common understanding of encryption and illuminated the false dichotomy that some have drawn between "security" and "privacy."[2] Security in the context of the encryption debate consists of multiple aspects including national security, public safety, cybersecurity and privacy, and security from hostile or oppressive state actors. The key is determining how to weigh competing security interests. The report therefore presents a framework of essential questions to evaluate plans for lawful access to encrypted data. In addition to the 2018 report, several computer scientists have proposed, albeit with controversy, design approaches they argue would allow access while using a variety of technical and procedural safeguards to minimize the increased risk to cybersecurity and prevent misuse. Finally, some governments have helpfully begun to acknowledge the difficulty of the problem and the downsides of requiring government access.[3] A recent article by UK officials, for example, highlights the lack of silver bullet solutions and therefore the need for principled collaboration and compromise.[4]

At the same time, disclosures of massive data breaches and revelations about the powerful user-tracking abilities of technology companies have underscored the valuable role encryption can play in safeguarding personal data.[5] Individuals around the world—from everyday citizens to at-risk groups such as journalists, activists, and marginalized groups fearing persecution—increasingly make use of encryption to protect not just against cyber crime but also unwanted disclosure and monitoring by technology platforms and other actors. The importance of encryption has grown as information technology enables the creation and storage of more and more sensitive personal information. User-

controlled encryption is and will be in the future an essential component of delivering on those desires, particularly as individuals become more skeptical of U.S.-based and foreign technology companies that would otherwise have access to sensitive private information. In addition, other countries have taken steps to strengthen data protection, such as the European Union General Data Protection Regulation (GDPR).

The group behind this paper—including former government officials, business representatives, privacy and civil rights advocates, law enforcement experts, and computer scientists—came together believing that more common ground is attainable and that the discussion can be best honed through specific, honest, and open-minded discussion among diverse perspectives. Our goals are:

(1) to engage in and promote a more pragmatic and constructive debate on the benefits and challenges of the increasing use of encryption;

(2) to identify specific areas where greater common ground may be possible; and

(3) to propose potentially more fruitful ways to evaluate the societal impact, including both benefits and risks, of any proposed approaches that address the impasse over law enforcement access to encrypted data.

We should highlight that we approach this issue from the point of view of stakeholders in the United States and discuss our framework for evaluating approaches in the U.S. context with policymakers at the national level as the target audience. The working group has sought not to repeat but rather to expand upon the 2018 NAS study. Although in many cases we reinforce some of the findings of the NAS study, our paper delves more deeply into one particular component of the debate—that on mobile phone encryption—and details a more specific approach to evaluating proposals focusing on law enforcement access to encrypted mobile phones.

We do so for two reasons. First, it is the problem set that is most commonly raised by law enforcement. However, importantly, we also found greater common ground and believe this is the area where a constructive dialogue is likely more achievable than other, even more contentious areas such as encrypted communication.

In this paper, we do not rule out any way forward regarding law enforcement access to encrypted mobile phones, nor do we endorse or propose any specific technical approach or legislation or mandates. Rather, we share what has shaped and emerged from our discussions: a framework for decisionmaking based on our findings about how to productively focus encryption considerations and debate, the core principles to which any proposed approach should adhere, and our approach to identifying and weighing risks through practical threat scenarios. These components have enabled

our group to find unanticipated agreement on some points, and we hope they will do the same for the broader debate over law enforcement access and encryption.

Pursuing a More Constructive Dialogue on Encryption and Law Enforcement Access

Many groups have published principles and key considerations related to the debate over law enforcement access to encrypted data. Each has helped advance the discussion by identifying key equities at stake, offering guidance for reaching agreement, or communicating the views of different groups. Rather than repeating or proposing replacing such content, we have set out several guidelines that can motivate better, healthier dialogue and avoid unproductive dead ends.

Avoid Absolutist Positions

All stakeholders should avoid holding absolutist positions; these are unlikely to result in productive dialogue. The focus should be on a careful and specific assessment of risks, benefits, trade-offs, and options. The goal must be to recognize, balance, and align core principles across a broad range of social and organizational interests. The United States and other liberal democratic governments are established, in part, to protect equality under the law as well as individual privacy and liberty. They are responsible for protecting the public safety and national security. They advance the economic interests of businesses and markets and carry out the full scope of a country's foreign policy. A more constructive debate requires continuing to deliver concurrently on all these promises: not by simply trading one for the other, but by seeking the best possible alignment of interests, as guided by shared principles and values.

Frame the Debate as a Shared Concern

Those who favor broad availability of strong encryption do not dispute that law enforcement is challenged by encrypted communications and devices and that in some instances strong encryption facilitates crime that harms real victims; those who favor lawful access do not dispute that use of strong encryption prevents crime and protects people. Stakeholders should seek out areas of common ground, establish shared interests, and consider and include the perspectives of all relevant stakeholder communities, not just a subset. Groups that are often underrepresented in this debate, including communities of color and low-income communities, bring valuable insights on how encryption policies could affect certain areas, for example, the disparate impacts of law enforcement and the impact on U.S. values of equality, openness, and privacy. Even within our group, we recognize that there are several such stakeholder communities that are not represented. We urge those who build upon our work to continue to expand engagement with these communities.

Recognize That Security Takes Many Forms and Is Intertwined With Privacy and Equity

"Security" can be defined in a variety of ways, such as national security and public safety, cybersecurity and privacy, or security from hostile or oppressive state actors. These interests are all priorities. All parties—including those who typically make rights-based arguments and those who typically make national security– and law enforcement–based arguments—are concerned with thwarting malicious actors, criminals, terrorists, and foreign agents, and investigating and preventing crime and threats to public safety. Encrypted technologies also support and enhance not only the speech and communications of individuals and communities but also the missions and operations of national security and law enforcement. The key is determining how we can jointly figure out how to weigh competing security responsibilities based on factual analysis and more informed cost/benefit assessments.

Assess the Range of Impacts

Privacy, cybersecurity, public safety, and national security are important, but they are not the sole interests at stake. Economic competitiveness, foreign policy, freedom of expression, civil and human rights, and the need to maintain an open internet are other important and sometimes overlapping interests. U.S. companies do business around the world. In addition, the U.S. economy *and* national security benefit from the U.S. technology advantage. Careful consideration is therefore warranted of whether any action might accelerate the loss of that advantage, especially in an environment where some nations and populations hold fairly antagonistic sentiments toward U.S. companies and manufacturers.

Attend to International Dynamics

While this paper focuses on the United States, the U.S. debate is not happening in a vacuum; it will affect (and be affected by) choices made in other countries and by non-U.S. technology companies. (Recent papers published by the Encryption Working Group assess the environment in Australia, Brazil, China, Germany, India, and the European Union.[6]) Any proposed approach should be adaptable beyond a U.S. setting, both to enhance commonality and to reduce the burden of implementation. Policymakers should consider the viability of any proposal in light of users and devices crossing borders. They should further consider that U.S. policies will give legitimacy to replication by other nations, including those with weaker judicial protections and records on human rights. Finally, policies should be considered in light of the effect they will have on U.S. foreign policy interests.

Think Long Term

Given rapidly changing technology and governmental needs, a long-term perspective is essential. Governments should account for technological change and recognize that needs will change over time. Industry, for its part, will innovate over time and in response to governance. Questions

including how encryption is likely to be deployed over time (based on evolving market trends, customer demand, and engineering realities) are important to consider, as is the continued rapid growth of digital data collection and storage.[7] Recent papers published by the Encryption Working Group, for example, examine the impact of quantum computing and likely future adoption of user-controlled encryption.[8]

Accept Imperfection

No approach will address every concern perfectly. Stakeholders must accept that some level of risk is inherent in any future path. Cybersecurity advocates should not dismiss out of hand the possibility of some level of increased security risk, just as law enforcement advocates should accept that they may not be able to access all of the data they seek. More conversations are needed to identify a reasonable standard of expectation in these areas, and whether precedents and existing standards (for example, those in the Electronic Communications Privacy Act, Wiretap Act, Foreign Intelligence Surveillance Act, or Fourth and Fifth Amendment jurisprudence) offer any guidance.

Separate the Debate Into Component Parts

It is probably impossible to establish a single approach that applies to each of the diverse applications of encryption in society. Stakeholders, technologies, processes, policies, and regulatory environments are very different when it comes to protecting data in the cloud, data in motion, and data on devices. Proposals that attempt to solve every issue are unlikely to succeed. The more constructive discussions will be those that examine one part at a time. Some components, as described in the next section, are more worthy of pursuit than others.

Place the Issue of Encryption Into the Broader Context of Law Enforcement Capabilities

Encryption has taken a central role in much of the public debate, but other policies and practices also affect law enforcement's ability to obtain data sought for investigations.[9] These include accessing data in the cloud and on internet-of-things devices, use of communications metadata, law enforcement hacking, obtaining timely and full compliance with court orders and other legal process in situations not involving encryption, as well as such legal and policy tools as mutual legal assistance treaties, personnel and resource levels, and policies on how government hacking is handled (for example, the vulnerabilities equities process). Investments in these areas could theoretically offset some of the impact on law enforcement from inaccessible encrypted data, but they also come with their own complex considerations and trade-offs.

Recognize There Is No Purely Technical Approach

Any proposal to increase law enforcement access must address process, infrastructure, and policy—not just technology. How would requests for access be made and authenticated? What would be the roles and responsibilities of various actors in the system? How would information be delivered? What sort of legal duties would law enforcement have to satisfy? What are the oversight expectations?

What would be the risks and benefits due to these nontechnical aspects? These kinds of nontechnical questions are necessary to understand fully any such proposal's risks and benefits.

Recognize the Challenge of Effective Implementation

A key principle of cybersecurity is to keep the design of systems as simple as possible; complexity highly increases the risk of insecurity. Any proposal should attempt to minimize the risk of catastrophic failures at the implementation level.[10]

Balance the Need for a Strategic Approach and the Need for Technical Detail

The world of cryptography, digital communications, and data management is deeply technical; this complicates the broader societal conversation that is needed on encryption. On one hand, more strategic, accessible approaches are needed to broaden this circle. On the other, some risks often can only be identified at very detailed, technical levels of investigation. Proposals should be tested multiple times—including at strategic levels (for example, do they establish high-level principles and requirements to weed out incomplete or unfeasible proposals?) and at technical levels (for example, what are the technical risks of the specific implementation?).

Produce Better Data for Both the Risks and Benefits of a Proposal

Many reports have lamented the inadequacy of available data to understand and evaluate the risks and benefits of proposals for law enforcement access to encrypted data. Agencies could adopt procedures to generate better data, such as tallies of how many encrypted devices they have encountered and in what types of cases. Structural challenges to producing the desired data require addressing the following questions: how can federal, state, and local law enforcement provide accurate data about investigations, or measure the quality of "leads" that came from such information? Similarly, how can stakeholders assess the degree to which a proposed solution is likely to result in a reduction in privacy for individuals, for example, who are not the intended targets of a lawful search? In other cases, such as understanding state- and local-level needs, the challenge is more about resources and authority to request such data. In any case, stakeholders in the encryption debate have an ongoing responsibility to reevaluate and seek better data to inform the debate.[11]

Starting Points

First of all, we reject two straw men—absolutist positions not actually held by serious participants, but sometimes used as caricatures of opponents—(1) that we should stop seeking approaches to enable access to encrypted information; or (2) that law enforcement will be unable to protect the public unless it can obtain access to all encrypted data through lawful process. We believe it is time to abandon these and other such straw men.

Specifically, systems exist today that allow for encryption as well as decrypted access by an authorized third party. (For example, some enterprise disk encryption products allow user control in most use cases, while enabling enterprise IT staff to recover data if necessary.) Does any approach deliver the important benefits of end-to-end encryption while addressing the various concerns noted above? That is a debate worth having. Can developers design systems with access for third parties? Yes. Should they be required to do so? There is significant disagreement in our group about that.

A position that law enforcement must have access to all information or else society will disintegrate is similarly lacking. Throughout modern history, there have been technologies to destroy information and there has been much information that was beyond the reach of law enforcement. The same is true today and society continues to function. And new sources of information are now available that did not exist or were not recorded in the past. Law enforcement has not shirked from its responsibility to catch criminals and reduce crime, nor will it in the future. Can law enforcement operate in an environment where encryption is more broadly available? Yes. Should law enforcement simply be required to cope with every possible type of encryption product? There is significant disagreement in our group about that.

Any approach serving the needs of persons or societies generally comprises a mix of technology, human action, and feedback mechanisms designed to ensure its proper operation. This is especially true of approaches proffered by governments, as in the case of the United States, based on a foundation of limited and constrained powers where the feedback mechanism must ensure that any approach taken, including a technological one, is constrained through procedures, controls, and oversight to the expressed purposes allowed by the Constitution and law of the United States. Therefore, we are likely to find that any approach seeking to align the various interests dependent on the use of encryption will comprise technology, procedures, and controls designed to deliver and sustain the desired alignment.

Focus on Mobile Phone Encryption Promises More Productive Discussion

Of all the guidance listed above, *separating the debate into its component parts* has been little embraced in practice. Few public statements from national governments, for example, have distinguished between approaches for data at rest and data in motion. Similarly, when groups raise concerns about undermining encryption, they tend to emphasize the general risks versus those related to specific applications of encryption.

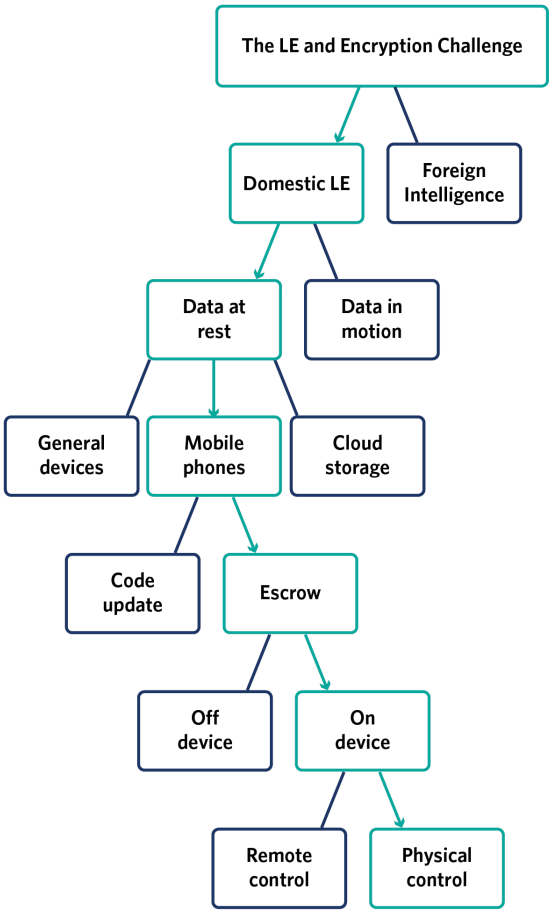
One exception has been the energetic debate in the cybersecurity research community about data at rest. Two computer scientists released separate preliminary approaches for how law enforcement might gain access to data stored on mobile phones while attempting not to undermine cybersecurity for all users.[12] Many in the computer security community are skeptical of these and similar approaches.[13] But whether or not these proposals stand up to rigorous testing and debate, at least they allow stakeholders to compare the risks and benefits of the same thing.

The working group encourages continued, focused dialogue on the topic of law enforcement access to mobile phone data at rest. We have not concluded that any existing proposal in this area is viable, that any future such proposals will ultimately prove viable, or that policy changes are advisable at this time. Rather, we urge continued, pragmatic debate on the topic. Mobile phone data at rest seems to us to be the area most likely to enable fruitful debate among diverse communities-of-interest and most likely to lead to clearer characterization of risks and benefits, for reasons we outline below and in Figure 1. Moreover, it is a good place to focus because if good-faith debate on all sides can't lead to more constructive discussions in this area, then there are likely none elsewhere.

Other parts of the encryption debate, as illustrated in Figure 1, seem much less tractable. In the case of data in motion, for example, our group could identify no approach to increasing law enforcement access that seemed reasonably promising to adequately balance all of the various concerns. For that reason, at least for now, this group believes that dialogue in this area will continue to be very difficult, and that implementing policy changes that give access to encrypted data in motion should not be pursued.

FIGURE 1

Focusing on Component Parts of the Law Enforcement (LE) and Encryption Challenge



Hypothetical Description of How Law Enforcement Access Might Look in Practice

The FBI arrests a suspect involved in a global money-laundering scheme. This individual has stored notes, documents, and other evidence associated with this activity on her phone. Some, but not all, of this information is only stored locally on her phone and not in cloud services accessible to the FBI through lawful process. The suspect, however, refuses to provide the password to unlock the phone. If law enforcement seeks to manually break the password, the phone will automatically wipe its contents, making the information permanently unobtainable. However, a decryption key specific to that phone alone that is retained physically on the phone, albeit currently inaccessible to law enforcement officials, would allow law enforcement to decrypt the contents of the phone. After

obtaining a warrant from a U.S. federal judge to access the decryption key, law enforcement officials then exercise a process authorized by the warrant to obtain the decryption key physically from that phone. This extracted information would allow the officials to directly read information on the phone and use it as evidence in the case against the suspect.

Branch 1: Focusing on the Domestic Law Enforcement Challenge Rather Than the Foreign Intelligence Challenge

The first branch in this decision tree excludes consideration of how the intelligence community accesses encrypted information targeted at non-U.S. persons outside the United States for the purpose of obtaining foreign intelligence information to understand foreign adversaries and their intentions. We think it is reasonable to assume that although the increasing use of encryption services may be a challenge for certain types of foreign intelligence collection abroad, it is likely not as acute as that for domestic law enforcement, which must operate within the context of the U.S. criminal justice system. (Agencies operating under intelligence rules, while restricted in certain ways, may have options that law enforcement agencies do not.)

Branch 2: Focusing on Data at Rest Rather Than Data in Motion

The second branch in this decision tree excludes, at this stage, consideration of approaches that would allow law enforcement access to data in motion (for example, text messages being exchanged through end-to-end encrypted messaging platforms). This is an area of significant importance to law enforcement agencies, which frequently cite encrypted data in motion, as occurs with texting applications such as WhatsApp, as a major challenge.

Data in motion poses challenges that are not present for data at rest. For example, modern cryptographic protocols for data in motion use a separate "session key" for each message, unrelated to the private/public key pairs used to initiate communication, to preserve the message's secrecy independent of other messages (consistent with a concept known as "forward secrecy"). While there are potential techniques for recording, escrowing, or otherwise allowing access to these session keys, by their nature, each would break forward secrecy and related concepts and would create a massive target for criminal and foreign intelligence adversaries. Any technical steps to simplify the collection or tracking of session keys, such as linking keys to other keys or storing keys after they are used, would represent a fundamental weakening of all the communications. Given this and other considerations, such as the number of independent keys in use, it is much harder to identify a potential solution to the problems identified regarding data in motion in a way that achieves a good balance.

Branch 3: Focusing on Encryption of Data on Mobile Phones Rather Than on Data on General Devices or in Cloud Storage

The third branch in this decision tree focuses on mobile phones. Ultimately, we decided to focus on mobile phones because that is what law enforcement agencies most commonly cite as the type of device to which they seek access. With that said, there are several other factors informing this decision. First, general devices—such as laptops, desktops, and workstations—provide users far more flexibility in configuring how and what software operates on the machine, making it less likely that a lawful access approach could be protected from work-arounds or compromise by criminal actors.[14] In addition, the great deal of variability between devices complicates any effort to design a lawful access system that would not unintentionally interfere with normal device functionality.

Law enforcement also relies on accessing, through appropriate legal process, encrypted data held in the cloud (like email, documents, calendar data, or contact information synchronized across devices). For law enforcement, however, this is a less worrisome area than encrypted phones or encrypted messaging. That is because providers often maintain access to encryption keys for data in the cloud in order to satisfy consumer needs to access, sync, and recover such data, for example when a password is lost. The prevalence of cloud data is growing and, as such, represents another tool and source of data for law enforcement. There is already significant work ongoing between law enforcement and technology providers to arrange the right procedures and capabilities to obtain such data through legal process.

Finally, mobile phones use commercial data services (for example, through cellular systems), unlike devices that lack that feature or connect to the network solely via Wi-Fi. The national cellular networks involve a relatively small number of companies operating under a national regulatory regime.[15] From a policymaking perspective, this may facilitate policy implementation. By contrast, a lawful access approach requiring action by the many types and locations of independently operated or owned local Wi-Fi services would be unmanageable.

Branch 4: Focusing on Approaches That Involve Key Escrow, Rather Than Delivery of Code Updates to a Phone

As scoped so far, there are two primary ways in which law enforcement could theoretically gain access to a mobile phone.[16] One of these is to develop an approach involving key escrow, in which copies of encryption keys are held securely so that, in certain circumstances, an authorized third party can access them. The second would be for law enforcement to ask or compel service providers to send a uniquely designed software update that would enable law enforcement to surreptitiously access data on a specific, targeted phone.

The working group has chosen to focus on key escrow approaches in part because code updates, typically delivered by service providers over the internet, patch known flaws in software and

hardware and are considered a foundation of basic cybersecurity hygiene. Companies and cybersecurity specialists worry that consumers will be less likely to accept updates—thus exposing themselves to exploitation by hackers and governments—if they are suspicious of potential government interventions through such means. Such disincentives, even if they only were to affect a percentage of users, would have a systemically negative impact on cybersecurity that could outweigh the benefits of lawful access. Another risk is that of unintended social distortions, for example, if minority groups who fear law enforcement targeting tend to decline updates more frequently than other users.

Another potential concern with code updates would be their potential detrimental impact on the expansion of nascent cybersecurity technologies, such as software and firmware transparency, that allow a user to confirm that they have received a standard update rather than one modified by hackers or law enforcement. These technologies benefit law-abiding users but would prevent the delivery of customized updates for a single phone on behalf of law enforcement from remaining a secret. Finally, from an operational perspective, the update approach may only be successful before an individual is aware that he is under law enforcement investigation. Once the individual is aware of an investigation or has been arrested, or the phone is taken into law enforcement custody, he is unlikely to accept further code updates.

However, advocates for code updates believe that they present a viable potential approach that, if done carefully and under lawful processes, could be a narrow and targeted way to obtain lawful access to data on encrypted phones. They also point to code updates that could be issued after the device has been lawfully seized. Advocates argue that the above assumptions regarding negative consumer behaviors in response to a code update system are not yet backed by empirical evidence.[17] They further argue that technologies such as software transparency are unlikely to be deployed widely. However, the group collectively agreed that its current efforts should focus on possible key escrow systems because of the unknowns and general disagreement regarding code updates.

Branch 5: Focusing on Key Escrow Arrangements Involving the Key Physically Residing on the Mobile Phone Device, Rather Than Off-Device

One of the characteristics that makes a focus on mobile phone encryption promising is the opportunity for the encryption key to physically reside on the mobile phone device, rather than off-device (for example, in a secured, but centralized, repository for a large number of such keys). Off-device key approaches increase cybersecurity risk in a way that makes achieving a good balance among equities less likely, largely because such a repository would be an attractive target that, if compromised, could constitute a single-point-of-failure of many (or even all) users at once. On-device escrow, on the other hand, can be implemented in ways that require physical access to the phone before the key can be recovered. This means that malicious actors might compromise phones in their possession but would not be able to compromise many phones en masse.

Branch 6: Focusing on Arrangements That Require Physical Control of the Phone in Order to Access the Key on the Phone Rather Than Using Remote Control

The final branch focuses on a system design that requires physical control of the device and excludes the possibility of remote access to the escrow key. A system that allows remote key recovery could allow an attacker to conduct an automated, systematic pillaging of the escrow repositories, making it no more secure than a centralized repository. In addition, technical or process mechanisms could better protect the escrow key from abuse, even in the event of physical control of the phone. For example, even if actors can collect the escrow package, its design would be to make it unreadable until protective encryption keys are gathered through a separate process.

Mobile Phone Proposals Should Be Evaluated Against Adherence to Core Principles

Having selected mobile phone encryption as a possible area for further analysis, the working group has identified core principles against which to judge proposals for mobile phone encryption access.[18] The group agrees that proposals should, at a minimum, adhere to these principles. In this, we drew first upon the principles outlined in Stefan Savage's paper, "Lawful Device Access Without Mass Surveillance Risk: A Technical Design Discussion,"[19] which the working group assessed were a good but incomplete start.[20] The working group suggests the following principles be used to judge both new technical proposals and any new policy or legislation that might be proposed. They are in no particular order, and their rank does not indicate one principle is more important than any of the others. (Note that these principles can and should be adapted to other component parts of the encryption debate, but we use them here in the context of mobile phone encryption.)

- Law Enforcement Utility: The proposal can meaningfully and predictably address a legitimate and demonstrated law enforcement problem.

- Equity: The proposal offers meaningful safeguards to ensure that it will not exacerbate existing disparities in law enforcement, including on the basis of race, ethnicity, class, religion, or gender.

- Specificity: The capability to access a given phone is only useful for accessing that phone (for example, there is no master secret key to use) and that there is no practical way to repurpose the capability for mass surveillance, even if some aspects of it are compromised.

- Focus: The capability is designed in a way that it does not appreciably decrease cybersecurity for the public at large, only for users subject to legitimate law enforcement access.

- Authorization: The use of this capability on a phone is only made available subject to duly authorized legal processes (for example, obtaining a warrant).

- Limitation: The legal standards that law enforcement must satisfy to obtain authorization to use this capability appropriately limit its scope, for example, with respect to the severity of the crime and the particularity of the search.[21]

- Auditability: When a phone is accessed, the action is auditable to enable proper oversight, and is eventually made transparent to the user (even if in a delayed fashion due to the need for law enforcement secrecy).

- Transparency, Evaluation, and Oversight: The use of the capability will be documented and publicly reported with sufficient rigor to facilitate accountability through ongoing evaluation and oversight by policymakers and the public.

Mobile Phone Proposals Should Be Tested Against a Variety of Use Cases to Clarify Risks and Benefits

Use cases—scenarios that help define the interactions between various actors and a system under consideration—are an important mechanism for identifying the feasibility, risks, and benefits of any given proposal. In this and other areas of the debate over law enforcement access to encrypted data, use cases can identify technical risk. More broadly, however, they are valuable to understanding the implications for sometimes under-addressed equities such as economic competitiveness, law enforcement conduct, and civil and human rights.

Some of the recent proposals have identified some of the cybersecurity-related threat scenarios.[22] However, we argue for a broader-based set of use cases that capture implications for vulnerable individuals and groups, economic competitiveness, international implementation, and more. In each of the following scenarios, the question is whether (1) the individual phone can be compromised and (2) how many phones can be compromised (scale). These scenarios are not comprehensive, but they illustrate generally applicable equities at stake for mobile phone proposals. In each case, analysis should consider how a particular approach would affect risks and benefits, compared to the status quo, under reasonable assumptions about engineering and user behavior.

Use Case 1: International Border

A border protection or foreign intelligence service, at the arrival or connection airport in their country, confiscates a traveler's mobile phone to seek access to its contents without relying upon the traveler's assistance.

> *Key questions: Could a foreign entity exploit or subvert the capability and proposed protections at an individual level? Would it provide new opportunities to subvert at scale?*

Use Case 2: Remote Access

Well-resourced, sophisticated remote hackers seek a work-around to gain access to encrypted phone on a massive scale.

> *Key questions: Is there an access point that would allow remote hackers to gain access to many phones? What is the estimated probability that sophisticated hackers could succeed in this?*

Use Case 3: Individual Misuse

An individual with malicious intent seeks to gain access to the contents of somebody else's phone in the former's possession, for example, in a marriage dispute.

> *Key questions: What protections are in place to prevent this individual from accessing the information on the phone, or from modifying applications/processes on someone else's phone? If the individual succeeded, would it compromise the single phone or many phones at scale?*

Use Case 4: Disabling by Criminal Suspect

A suspect, facing arrest, seeks to prevent law enforcement from accessing the contents on her phone or phones.

> *Key questions: What would it take to prevent law enforcement from accessing the phone's contents? Would enough users have access to the means to undertake this to undermine the benefit to law enforcement? Would the suspects of most interest to law enforcement develop this capability?*

Use Case 5: Supply Chain

An adversarial foreign government seeks to insert compromised hardware or software onto one or more mobile phones to defeat security protections.

> *Key questions: Which components would need to be compromised, and how likely is this? Could it defeat protections on individual phones or allow subversion on a large scale?*

Use Case 6: Insider Threat

An individual with special access (for example, from inside the phone manufacturer, service provider, or law enforcement) seeks to subvert the proposed system.

> *Key questions: Could such an individual compromise, or provide others (for example, a nation state) the opportunity to compromise the system on an individual scale? On a massive scale?*

Use Case 7: Local Policing Impacts

The proposed access mechanism becomes readily available not just at the national (FBI) level but also at the local law enforcement level.[23]

> *Key questions: What are the challenges of scale? Will the capability be equally available to all jurisdictions? Will the capability be implemented in a distributed or centralized manner, and how would cybersecurity and auditing be handled in either case? How likely is it that the use of the capability by local law enforcement will exacerbate racial inequities in policing? How easy or difficult will it be for local law enforcement to gain the necessary legal authority to use the capability? What policies or other procedural safeguards will be in place to ensure that individual civil and constitutional rights are protected? How easy or difficult will it be for local law enforcement to gain the necessary technical expertise to employ this capability?*

Use Case 8: Technology Competition

Phones made by tech companies are required to implement the proposed system in the United States.

> *Key questions: What are the likely impacts on competitiveness of U.S. companies? How would U.S. companies be impacted by contradictory legal requirements in different jurisdictions? To what extent might U.S. companies be disadvantaged in the market?*

Use Case 9: Human and Civil Rights Impacts

A repressive regime seeks to access data on target phones without undertaking legitimate legal process.[24]

> *Key questions: To what extent would there be protections against such a scenario? If a repressive regime gains access, what could the consequences be for vulnerable individuals, such as a human rights activist?*

Conclusion: Some Paths Are More Tractable Than Others

There will be no single approach for requests for lawful access that can be applied to every technology or means of communication. More work is necessary, such as that initiated in this paper, to separate the debate into its component parts, examine risks and benefits in greater granularity, and seek better data to inform the debate. Based on our attempt to do this for one particular area, the working group believes that some forms of access to encrypted information, such as access to data at rest on mobile phones, should be further discussed. If we cannot have a constructive dialogue in that easiest of cases, then there is likely none to be had with respect to any of the other areas. Other forms of access to encrypted information, including encrypted data-in-motion, may not offer an achievable balance of risk vs. benefit, and as such are not worth pursuing and should not be the subject of policy changes, at least for now. We believe that to be productive, any approach must separate the issue into its component parts.

Acknowledgments

The Encryption Working Group wishes to thank the outside reviewers who provided comments on earlier drafts of this paper. The reviewers provided valuable feedback, however they were not asked to endorse the paper nor did they see the final paper before its release. We thank Steve Bellovin, Scott Charney, Mieke Eoyang, Paul Figueroa, Jerome Greco, Ian Levy, Herb Lin, Chris Magnus, Kate Martin, Paul Ohm, Chris Riley, and Peter Weinberger. Several additional reviewers wished to remain anonymous. The working group also thanks staff and researchers at the Carnegie Endowment for International Peace and Princeton University's Center for Information Technology Policy, in particular Rachel Osnos, Mona Damian, and the Carnegie communications team. We are especially grateful for the outstanding contributions of Garrett Hinck, Kathryn Taylor, and Jenny Wang in making the working group and this paper possible. Responsibility for the final content rests entirely with the Encryption Working Group and does not represent the institutional views of any of the affiliations of its members.

Notes

[1] Law enforcement officials tend to use the term "mobile devices" in this debate. We refer to "mobile phones" in this paper to avoid potential confusion with other devices such as tablets.

[2] National Academy of Sciences. 'Decrypting the Encryption Debate: A Framework for Decision Makers' (2018) https://www.nap.edu/read/25010/chapter/1

[3] This is not universally the case, though, as some have criticized the Australian approach as excessively broad.

[4] Ian Levy and Crispin Robinson. "Principles for a More Informed Exceptional Access Debate." (Lawfare, November 29, 2018), https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate

[5] While encryption can safeguard personal data, it is important to note that it does not affect other means to collect data on a person such as, for example, metadata analysis. The broader goal of improving systemic cybersecurity will require efforts from law enforcement, the private sector, and other key actors—and as such is beyond the scope of this paper.

[6] These briefings can be found under "The Encryption Debate Internationally" on the page for the Encryption Working Group, Carnegie Endowment for International Peace, 2019. https://carnegieendowment.org/programs/technology/cyber/encryption

[7] For a view to how evolving market trends will shape the deployment of encryption, refer to the working group's paper "Likely Future Adoption of User-Controlled Encryption," and for a view of how quantum technology will affect encryption, see the briefing on "Implications of Quantum Computing for Encryption Policy."

[8] These briefings can be found under "Future Trends on the Encryption Working Group website. https://carnegieendowment.org/programs/technology/cyber/encryption

[9] Recent reform efforts with respect to Mutual Legal Assistance Treaties, namely the Cloud Act, are also worth mentioning here.

[10] A good analogy to use is to think of implementing a complex security mechanism as building a house in a flood zone. You know that every so often it will get flooded, and you plan accordingly. Or if never being flooded is important, you don't build in a flood zone.

[11] Examples of potentially useful data includes volume / proportion of data and devices that law enforcement cannot access at one point in time compared to devices that law enforcement can access successfully; the type of crime being investigated; the available alternatives for accessing data; the specific types of content that law enforcement wants to access; specific understanding of which data is and is not available from which providers under default settings as it relates to investigations, and how different segments of users will alter their behavior in response to any proposed approach.

[12] Ray Ozzie, "CLEAR," January 2017, https://github.com/rayozzie/clear/blob/master/clear-rozzie.pdf Also see Steven Levy, "Cracking the Crypto War," *WIRED,* April 25, 2018, https://www.wired.com/story/crypto-war-clear-encryption/
Stefan Savage, "Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion," *Proceedings of the ACM Conference on Computer and Communications Security,* Toronto, Canada, October 2018.

[13] Steven M. Bellovin, Matt Blaze, Dan Boneh, Susan Landau, and Ronald L. Rivest, "Analysis of the CLEAR Protocol per the National Academies Framework," https://mice.cs.columbia.edu/getTechreport.php?techreportID=1637
Eran Tromer, "Eran Tromer's Attack on Ray Ozzie's CLEAR Protocol," Steve Bellovin Blog, May 2, 2018. https://www.cs.columbia.edu/~smb/blog/2018-05/2018-05-02.html

[14] Similarly, we note that the ease with which much software, and especially open source software, can be modified also complicate attempts to mandate law enforcement access to encrypted data. We do not attempt a more detailed discussion of these issues in this paper.

[15] Note, though, that there are already mass market Wi-Fi-only small mobile devices including phones and tablets. The next set of networked in-home devices will use Wi-Fi, not cell data. Requiring all cellular-accessible devices to be compliant with lawful access requirements could result in a further increase in the type and variety of Wi-Fi-only communication devices.

[16] An alternative option would be for law enforcement to attempt to use hacking capabilities, including potentially purchasing such capabilities from private companies, to obtain access to individual phones. Although the issue of law enforcement hacking is not the subject of this paper, it should be acknowledged as a part of the broader debate about law enforcement access in general. For more background, see : Steven Bellovin, Matthew Blaze, Sandy Clark, Susan Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," *Northwestern Journal of Technology and Intellectual Property* Vol. 12, Issue 1 (2014).

[17] Existing studies have looked at the likelihood that users will accept future updates based on their past experiences with design changes, but have not surveyed users about cybersecurity concerns related to updates. For a discussion of user attitudes toward Windows updates see Kamia Vaniea, Emily Rader, Rick Walsh, "Betrayed by Updates: How Negative Experiences Affect Future Security," Proceedings of the SIGCHI Conference on Human Factors in Computer Systems, 2014. https://bitlab.cas.msu.edu/papers/itunes.pdf
For a discussion of user perceptions of the costs of updates, see Francesco Vitale, Joanna Mcgrenere, Aurélien Tabard, Michel Beaudouin-Lafon, Wendy Mackay. High Costs and Small Benefits: A Field Study of How Users Experience Operating System Upgrades. CHI 2017, May 2017, Denver, United States. ACM, pp. 4242-4253 2017, Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. https://chi2017.acm.org/. Doi: 10.1145/3025453.3025509

[18] We use the term "proposal" quite broadly, to be inclusive of technical proposals or policy/legislative-level proposals. In either case, we should judge such proposals by their attention to and ability to accommodate/enable the principles laid out in this section. We also focus here on proposals for access to encryption, but the working group has ruled out neither proposals that would instead prohibit or otherwise restrict such access, nor the possibility of retaining the status quo.

[19] Stefan Savage, "Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion," *Proceedings of the ACM Conference on Computer and Communications Security,* Toronto, Canada, October 2018, http://cseweb.ucsd.edu/~savage/papers/lawful.pdf

[20] The principle authorization was adapted directly from Stefan Savage's paper. Savage's principle of "non-scalability" was combined with particularity and modified. Savage's principle of "transparency" was modified to "auditability" to reflect the need for law enforcement actions to occasionally involve delayed transparency due to secrecy requirements. The remaining three principles of beneficial, equitable, and targeted were added by the working group to fill gaps.

[21] Consider similar discussions about the scope of Title III wiretaps, for example.

[22] For instance, Stefan Savage's paper noted two broad categories of threats. First, the risk of unauthorized actors gaining access to a single device using a security vulnerability introduced into the system by the access mechanism. Second, the risk of an unauthorized actor bypassing the system design to access a large number of devices remotely and covertly for the purpose of mass surveillance.

[23] This paper focuses on the United States. This particular use case will differ significantly in other countries.

[24] For a real-world example of this scenario, see Raymond Zhong, "China Snares Tourists' Phones in Surveillance Dragnet by Adding Secret App," *New York Times,* July 2, 2019. https://www.nytimes.com/2019/07/02/technology/china-xinjiang-app.html

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org