Consensus Study Report
HIGHLIGHTS

February 2018

Decrypting the Encryption Debate:

A Framework for Decision Makers

Encryption, confined until the Internet era to sensitive government and commercial transactions, has become widely available to the public. Today, encryption protects information stored on smartphones, laptops, and other devices belonging to hundreds of millions of users. Individuals, organizations, and governments rely on encryption to counter threats from a wide range of actors, including both sophisticated and unsophisticated criminals, foreign intelligence agencies, and repressive governments. At the same time, some criminals rely on encryption to prevent investigators from accessing the contents of locked smartphones or encrypted messages.

Although law enforcement and intelligence agencies were once able to rely on court orders and subpoenas to access data directly from technology vendors and service providers, this path is no longer available in cases where these third parties do not hold the necessary encryption keys. To address this issue, law enforcement and some intelligence officials have increasingly called for a reliable way to access unencrypted data so that they can fulfill their public safety and national security missions. They point to the widespread use of encryption in common products and services, national security threats posed by terrorist groups and foreign rivals, and the growing importance of digital evidence in a world where human activity is increasingly digital. Critics have objected to proposals for regulations to ensure government access to encrypted information on a number of legal and practical grounds, arguing that they would be ineffective, pose unacceptable risks to cybersecurity and privacy, disadvantage U.S. providers of products and services, and hamper innovation in encryption technologies.

To better inform future decision making and the policy debate, the National Academies of Sciences, Engineering, and Medicine organized a study to examine the options and tradeoffs associated with providing government agencies access to encrypted information. The resulting report, *Decrypting the Encryption Debate: A Framework for Decision Makers*, describes how encryption is used for cybersecurity and to protect civil liberties, explores technical and policy options for accessing plaintext, and reviews the needs of law enforcement. The report does not seek to answer the question of whether access mechanisms should be required, but rather presents a framework for evaluating policy or technical approaches to highlight key issues and guide future decisions.

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

LEGAL AND TECHNICAL OPTIONS

There is a wide variety of legal and technical options available to governments that seek access to plaintext for law enforcement and intelligence investigations. These include the following:

- Take no legislative action to regulate the use of encryption, but potentially pursue technical, law enforcement, and legal options to obtain or compel cooperation of the target.
- Provide law enforcement with additional resources to access plaintext.
- Enact legislation that requires device vendors or service providers to provide government access to plaintext without specifying the technical means of doing so
- Enact legislation requiring a particular technical approach

Some computer scientists have reacted with concern to renewed proposals to regulate the use of encryption, citing the security risks. Several attempts have been made in recent years to come up with technical mechanisms to provide the government with exceptional access to encrypted data in a way that would minimize these risks; the report offers a framework that can be used to evaluate such proposals.

QUESTIONS FOR DECISION MAKERS

The report offers a framework as a set of questions to ask about any path forward on encryption policy. The objective of this framework is not simply to help policy makers determine whether a particular approach is optimal or desirable, but also to help maximize the effectiveness and minimize the harmful side effects of any approach under consideration. The questions are as follows:

1. To what extent will the proposed approach be effective in permitting law enforcement and/or the intelligence community to access plaintext at or near the scale, timeliness, and reliability that proponents seek?
2. To what extent will the proposed approach affect the security of the type of data or device to which access would be required, as well as cybersecurity more broadly?
3. To what extent will the proposed approach affect the privacy, civil liberties, and human rights of targeted individuals and groups?
4. To what extent will the proposed approach affect commerce, economic competitiveness, and innovation?
5. To what extent will financial costs be imposed by the proposed approach, and who will bear them?
6. To what extent is the proposed approach consistent with existing law and other government priorities?
7. To what extent will the international context affect the proposed approach, and what will be the impact of the proposed approach internationally?
8. To what extent will the proposed approach be subject to effective ongoing evaluation and oversight?

FACTORS TO CONSIDER

In addressing these questions, policy makers will have to contend with incomplete data about the impact of encryption on investigations as well as incomplete data about the deliberate use of encryption by criminals. It is also difficult to quantify key factors such as the additional security risks of adding exceptional access to encryption systems. There are also a number of cases where one can only speculate about future behaviors that have bearing on the implications of government regulation of encryption. These include the fraction of criminals that would use noncompliant, unbreakable encryption if the government were to require vendors to provide exceptional access and the fraction of foreign customers that would eschew U.S. products if exceptional access were required.

Policy makers will also have to contend with the tradeoffs associated with encryption and government access that underlie these questions. Adding an exceptional access capability to encryption schemes would weaken their security to some degree, while the absence of an exceptional access mechanism would hamper government investigations to some degree. How much security is reduced and whether the resulting level of security remains acceptable depends on the specific technical and operational details and on the requirements and perspectives of users. The impact on society when an investigation is hindered or thwarted will depend on the scope and scale of the associated crime or national security threat.

There are no easy answers and many uncertainties in responding to these questions. However, developing and debating answers to these questions will help illuminate the underlying issues and tradeoffs and help inform the debate over government access to plaintext.

COMMITTEE ON LAW ENFORCEMENT AND INTELLIGENCE ACCESS TO PLAINTEXT INFORMATION: Fred H. Cate, Indiana University, Chair; Dan Boneh, Stanford University; Frederick R. Chang, Southern Methodist University; Scott Charney, Microsoft Corp.; Shafrira Goldwasser, Massachusetts Institute of Technology; David A. Hoffman, Intel Corporation; Seny Kamara, Brown University; David Kris, Culper Partners, LLC; Susan Landau, Tufts University; Steven B. Lipner, SAFECode; Richard Littlehale, Tennessee Bureau of Investigation; Kate Martin, Center for American Progress; Harvey Rishikof, Cybersecurity Legal Task Force, American Bar Association; Peter J. Weinberger, Google, Inc.

STAFF: Jon Eisenberg, Study Director and Senior Director, Computer Science and Telecommunications Board; Katiria Ortiz, Associate Program Officer; Shenae Bradley, Administrative Assistant; Janki Patel, Senior Program Assistant

This Consensus Study Report Highlights was prepared by the Computer Science and Telecommunications Board based on the report *Decrypting the Encryption Debate: A Framework for Decision Makers* (2018). The study was sponsored by the William and Flora Hewlett Foundation, the John D. and Catherine T. MacArthur Foundation, and the National Science Foundation. Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of the sponsors. Download the report at **nap.edu** and learn more about the board at **nas.edu/cstb**.

Division on Engineering and Physical Sciences

The National Academies of
SCIENCES · ENGINEERING · MEDICINE

The nation turns to the National Academies
of Sciences, Engineering, and Medicine for
independent, objective advice on issues that
affect people's lives worldwide.
www.national-academies.org