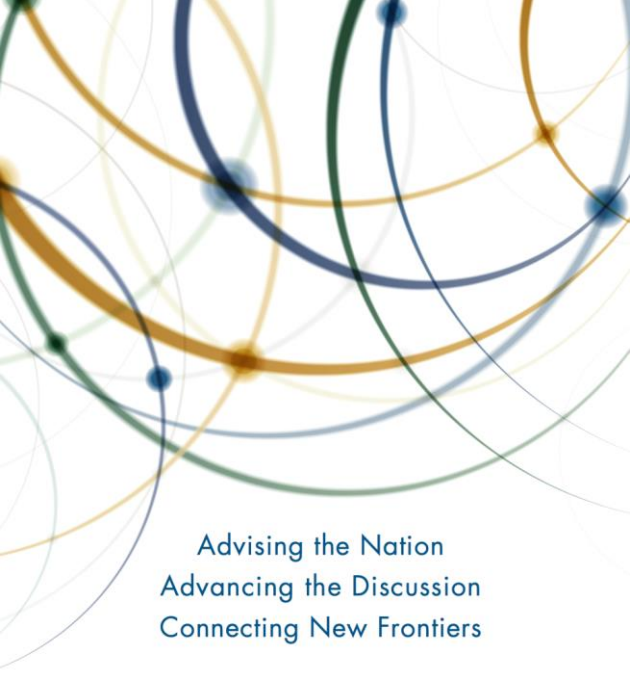
Decrypting the Encryption Debate

A Framework for Decision Makers

The National Academies of SCIENCES ENGINEERING MEDICINE

nap.edu/25010



The **National Academy of Sciences**, **National Academy of Engineering**, and **National Academy of Medicine** work together as the **National Academies of Sciences, Engineering, and Medicine** to provide independent, objective analysis and advice to the nation and conduct other activities to solve complex problems and inform public policy decisions.

Charge and Approach

Charge

- Examine the tradeoffs associated with mechanisms to provide authorized government agencies with access to the plaintext version of encrypted information
- Analyze options and trade-offs
- (No recommendations)

Approach

- Explore legal and technical options available to governments
- Provide a framework (in the form of a set of questions) to ask about any path forward

Sponsors

- William and Flora Hewlett Foundation
- John D. and Catherine T. MacArthur Foundation
- National Science Foundation

Any opinions, findings, or conclusions expressed in this presentation do not necessarily reflect the views of any organization or agency that provided support for the project.

Committee

Fred H. Cate, Indiana Univ., *Chair*

Dan Boneh (NAE), Stanford Univ.

Frederick R. Chang (NAE), Southern Methodist Univ.

Scott Charney, Microsoft Corp.

Shafrira Goldwasser (NAS, NAE), MIT

David Hoffman, Intel Corp.

Seny Kamara, Brown Univ.

David Kris, Culper Partners LLC

Susan Landau, Tufts Univ.

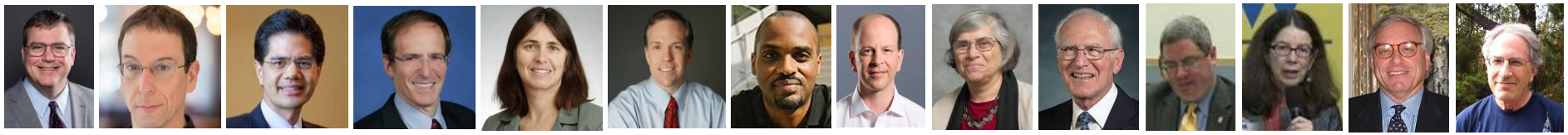
Steven B. Lipner (NAE), SAFECode

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.



The Report

Summary

Chapter 1. Introduction

Chapter 2. Encryption and Its Applications

Chapter 3. The Role of Encryption in Protecting Privacy and Civil Liberties

Chapter 4. Information Needs of Law Enforcement and the Intelligence Community

Chapter 5. Options for Accessing Plaintext

Chapter 6. International Dimensions

Chapter 7. A Framework for Evaluating Approaches to Access Plaintext

Context

- Smartphones and messaging applications make encryption available (by default) to many hundreds of millions of users
  - Vendors and service providers do not have access to the keys
- Encryption is an important (but not sufficient) tool for protecting data and systems
- Encryption is relied on by
  - Individuals, organizations, and governments to counter threats from a wide range of actors including criminals, foreign intelligence agencies, and repressive governments
  - By criminals and others to avoid investigation and prosecution
- Encryption complicates law enforcement and intelligence investigations
  - Intercepted messages cannot be understood if communications are encrypted end-to-end
  - Contents of a smartphone cannot be read when it is locked and encrypted

The Law Enforcement Argument

Law enforcement and some intelligence officials call for a reliable and sufficiently rapid and scalable way to access plaintext (decrypted data and messages) so that they can **protect the public and fulfill their public safety and national security missions**

- Widespread and increasing use of encryption by default in widely used products and services
- National security threats posed by terrorist groups and foreign rivals
- The increasing importance of digital evidence as human activity and crime have become increasingly digital
- The limited effectiveness of alternative sources of digital evidence

Legal and Practical Objections

Regulations to ensure government access to plaintext likely would:

- Be ineffective
- Pose unacceptable risks to cybersecurity
- Pose unacceptable risks to privacy and civil liberties
- Disadvantage U.S. providers of products and services
- Hamper innovation in encryption technologies
- May be less necessary in light of the wider availability of data—and especially metadata—generally, and the alternative means currently available to obtain access to encrypted data

Responses from the Technical Community

- Some computer scientists have reacted with concern to renewed proposals to regulate the use of encryption, citing the security risks

- Several recent attempts have also been made to come up with technical mechanisms that would minimize these risks. Three were presented to the committee during its work
- These proposals have not been fully fleshed out, tested, or deployed. But the committee did use them to help develop and test its framework for evaluating suggested approaches

Legal and Technical Options

- Take no legislative action to regulate the use of encryption
- Provide law enforcement with additional resources to access plaintext
- Enact legislation that requires that device vendors or service providers provide government access to plaintext without specifying the technical means of doing so
- Enact legislation requiring a particular technical approach

How to choose among these options and evaluate specific proposals?

Data Limitations and Uncertainties

- Incomplete data on impact on law enforcement
  - Data not collected uniformly
  - Does not address impact of encryption on investigations
  - Little data on extent of deliberate use of encryption by criminals
- Limited ability to measure additional security risks given difficulty measuring risk at all
- Necessarily speculative projections about future behavior
  - Fraction of criminals that would use noncompliant, unbreakable encryption
  - Fraction of foreign customers that would eschew U.S. products
- Complexity
  - Thousands of products and services in global market
  - Interactions of those markets with the strategies and policies that are adopted by other nations

A Fundamental Tradeoff

Adding an exceptional access (EA) capability to encryption schemes necessarily weakens their security to some degree, while the absence of an EA mechanism necessarily hampers government investigations to some degree

- How much security is reduced and whether the resulting level of security remains acceptable depend on the specific technical and operational details of the EA mechanism 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

A Framework (8 Questions) for Considering Any Path Forward

- Help policy makers determine whether a particular approach is desirable
- Help ensure that any approach that policy makers might pursue is implemented in a way that maximizes its effectiveness while minimizing harmful side effects
- Caveat: There are unlikely to be options that satisfy everyone, and solutions will be, at best, only partially effective

Applications of the Framework

- **Regulatory requirements**, such as a general requirement that the manufacturers of a particular device must ensure lawful access to that device
- **Policy choices**, such as a decision to provide more funding to support efforts by government agencies to obtain lawful access to plaintext
- **Particular technologies** or system modifications that might be imposed by law or implemented in response to a general requirement for access

The questions that follow use "**approach**" for all of these

Framework Questions

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 others**?
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**?

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?

- Does it work?
- At what scale, timeliness, and reliability?
- Does this meet the proponent's objectives?
- How long will be be effective in the face of rapid technological change?

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**?

- What is the impact on security
  - In the context of the particular type of service or device?
  - More broadly?
- What the potential scale at which the approach could be compromised?
- How would one detect compromise?
- How would one recover from compromise?

3. To what extent will the proposed approach affect the **privacy, civil liberties, and human rights** of **targeted individuals and others**?

- With respect to targeted individuals, how well does it ensure that government access will only be
  - permitted with appropriate authorization?
  - only to the content specifically authorized?
- With respect to people not targeted,
  - How does the approach guard against unauthorized surveillance?
  - Will it be used so widely as to chill free expression/association?

4. To what extent will the proposed approach affect **commerce, economic competitiveness, and innovation**?

- What will be the effect on the competitiveness of U.S. vendors and service providers?
  - Will it limit the ability of US. firms to market products and services as "secure"?
- How will the approach affect R&D and the deployment of innovative products and services?

5. To what extent will **financial costs** be imposed by the proposed approach, and **who will bear them**?

- How large are the total costs, including design, implementation, operational, compliance, and oversight costs?
- How will those costs be distributed across industry, individuals, and governments?

6. To what extent is the proposed approach **consistent with existing law and other government priorities**?

- Is the approach consistent with
  - Relevant legal requirements?
  - Other/broader government objectives, such as freedom of expression and association?
  - Objectives of U.S. foreign policy?
- Do unsettled questions of law make the approach more challenging or otherwise less attractive?

7. To what extent will the **international context** affect the proposed approach, and what will be the **impact of the proposed approach internationally**?

- What effects would the approach have on
  - International trade?
  - U.S. foreign policy objectives?
  - U.S. nationals travelling abroad?
  - Existing international agreements around privacy and cybersecurity?
- What impact might international developments have on the effectiveness of the approach?
  - Will enforcement be practical if nonconforming products and services are available globally?
  - What if any enforcement will be necessary at border crossings?

8. To what extent will the proposed approach be subject to **effective ongoing evaluation and oversight**?

- How will the approach
  - Be subject to effective and continuing evaluation and oversight?
  - Include audit mechanisms to detect misuse and unintended consequences?
- Will the proposed oversight mechanisms be sufficiently reliable, robust, and effective?

Concluding Thoughts

- No easy answers to and many uncertainties in responding to the questions
- Developing and debating answers to these questions will help illuminate the underlying issues and trade-offs and help inform the debate over government access to plaintext
- Report offers an analytical framework together with a common vocabulary and context.
- We hope this will facilitate an ongoing, frank conversation, involving diverse parties

Full report available at https://nap.edu/25010