CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

PRINCETON UNIVERSITY

CITP CENTER FOR INFORMATION TECHNOLOGY POLICY

Key Takeaways from the Encryption Working Group's Paper on "Moving the Encryption Policy Conversation Forward"

This document summarizes the paper by the Encryption Working Group to move the encryption policy debate forward. 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.

The group specifically aims 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. "Moving the Encryption Policy Conversation Forward" 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.

KEY TAKEAWAYS

The working group rejects two straw men—absolutist positions not actually held by serious participants, but sometimes used as caricatures of opponents. These are:

- (1) that we should stop seeking approaches to enable access to encrypted information
- (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.

More work is necessary, such as that initiated in this paper, to separate the debate into its component parts and examine risks and benefits in greater granularity.

- There will be no single approach for requests for lawful access that can be applied to every technology or means of communication.

- 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.

The working group encourages continued, focused dialogue on the topic of law enforcement access to mobile phone data at rest.

- 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.
- 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.
- If good-faith debate on all sides can't lead to more constructive discussions in this area, then there will likely be none elsewhere.

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.

MOBILE PHONE PROPOSALS SHOULD BE EVALUATED AGAINST ADHERENCE TO CORE PRINCIPLES

The working group has identified core principles against which to judge proposals for mobile phone encryption access. The group agrees that proposals should, at a minimum, adhere to these principles.

- **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.
- **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. The working group offers a set of use cases (relating to international borders, remote access, individual misuse, disabling by a criminal suspect, supply chain, insider threat, local policing impacts, technology competition, and human and civil rights impacts) to clarify risks and benefits of any approach.

We urge others to build upon this work. This includes continuing to expand engagement with underrepresented communities within the debate, such as communities of color and low-income communities.

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