EastWest INSTITUTE

Encryption Policy in Democratic Regimes

Finding Convergent Paths and Balanced Solutions

EXECUTIVE SUMMARY

Read the full report at
eastwest.ngo/encryption

The EastWest Institute works to reduce international conflict, addressing seemingly intractable problems that threaten world security and stability. We forge new connections and build trust among global leaders and influencers, help create practical new ideas, and take action through our network of global decision-makers. Independent and nonprofit since our founding in 1980, we have offices in New York, Brussels, Moscow and San Francisco.

The EastWest Institute
708 Third Avenue, Suite 1105
New York, NY 10017 U.S.A.
+1-212-824-4100

communications@eastwest.ngo
www.eastwest.ngo

▶ An electronic version of this report is available at: **www.eastwest.ngo/encryption**.

Executive Summary

Encryption is an essential tool for protecting digital data and communications. It supports privacy and other human rights, protects financial assets and proprietary data, enhances national security and thwarts cyber-enabled crime.

Long used by banks and governments, encryption's increasing use in business and by individuals is fueled by multiple developments, including the theft of business data and liabilities associated with data breaches, state surveillance of communication networks and the decisions of major information and communications technology (ICT) companies to provide strong, user-friendly encryption by default. However, the widespread use of encryption reduces law enforcement's ability to access vital digital evidence and other critical information to fight crime. Some governments are responding to this "going dark" problem by considering restricting the availability or effectiveness of commercial encryption products and services. Opponents of such controls emphasize the substantial benefits of encryption and argue that the increasing connectivity and digitization of public and private life compensate for the loss of access and may herald the dawn of a "golden age of surveillance" for law enforcement.

Proposals to provide lawful access to plaintext[1] often lead to acrimonious discussions, with each side becoming entrenched, and yielding little constructive progress. Therefore, the EastWest Institute (EWI) has set out to identify and explore middle-ground proposals that acknowledge encryption's dual nature and that could feasibly be agreed upon and implemented on an international basis, at least among democratic governments. This report proposes two balanced, risk-informed, middle-ground encryption policy regimes in support of more constructive dialogue. The proposed regimes would enable legally authorized law enforcement access to the plaintext of encrypted data in limited cases and within a clear legal framework embedded with human rights safeguards. At the same time, the proposed regimes attempt to mitigate the risk that third parties could gain unauthorized access and breach the confidentiality of the encrypted data and communications.

The global nature of the digital environment means that any national solution will be neither sufficient nor comprehensive. Even among democracies, where costs and benefits are balanced through public and political processes, differing cultural values and legal traditions will drive different approaches. Cross-border cooperation among law enforcement entities and compliance by global companies with multiple, differing national requirements will remain challenging features in the global cyber landscape.

Recommendations

The report provides nine normative recommendations on encryption policy for lawful law enforcement access regarding crime and terrorism prevention, investigation and prosecution.[2] This section summarizes the recommendations; a more detailed discussion may be found in Section 6. The recommendations help to advise the formulation of specific policies; recommendations 1 through 3 and 9 are generally applicable, whereas recommendations 4 through 8 are relevant to specific policies or issues.

1) Strong Cybersecurity. Governments must support and enable strong encryption and other digital protections to promote strong cybersecurity. Governments must refrain

1 The report uses the word "plaintext" to include data in any form that is not encrypted, including audio, video, images and sensor data.

2 The report generally avoids addressing access to data for national security purposes by military and intelligence authorities. Rather, the focus of the report is on access to encrypted data with regard to prevention, investigation and prosecution of crime and terrorism and the respective challenges encountered by law enforcement and the judiciary.

from policies and measures that systematically and broadly undermine cybersecurity for all users. Yet, targeted, specific measures that enable access to unencrypted data may be permissible under principled considerations.

2) Balanced, Transparent, Risk-Informed Regimes. Governments must create balanced, transparent and risk-informed regimes for encryption policy that govern law enforcement access to encrypted data. These regimes must reflect considered trade-offs among the government (including law enforcement, justice, national security, cybersecurity, economic and social well-being, and public safety), businesses (including administrative burden and compliance costs), the economy (including impacts on the industry's innovation and competitiveness) and civil society (including the protection of privacy and other human rights) and must be a result of a process embedded in democratic institutions.

3) Systemic Improvements. Governments must undertake systemic improvements to the state's legal, organizational and technical infrastructure to strengthen law enforcement's and the judiciary's capabilities to effectively and efficiently detect, prevent, investigate and prosecute crime and terrorism that depends on and/or is facilitated by cyber means, and to reduce the need for direct regulation of encryption (e.g., prohibiting or restricting the development and use of encryption technology).

4) Clear Rules on Compelled Provider Assistance. Governments should use compelled provider assistance as a fundamental approach to facilitate law enforcement access, but only with clear rules as to where and to what extent compelled provider assistance is applicable under the legal framework. Requests for compelled provider assistance must be targeted and limited to a particular case. Compelled assistance should be the preferred technique to facilitate lawful access to third-party encryption products, services and ephemeral communications.

5) Limitations on Lawful Hacking. Governments must recognize lawful hacking as a tool for use only in extraordinary circumstances, particularly when used for remote or extraterritorial applications. Lawful hacking must be embedded in a strict legal framework with limitations on its use to the most serious cases (i.e., testing the application against the principles of proportionality, necessity and legality, assessing international and human rights implications), and be subject to comprehensive vulnerability management, independent judicial authorization and oversight, and public summary reporting to the legislature. Effective state-of-the-art safeguards to prevent loss or theft of lawful hacking tools and the vulnerabilities they utilize must be deployed.

6) Limitations on Design Mandates. Design mandates that require service providers and device manufacturers to retain capabilities to produce decrypted data must be limited to designated services and scope. Design mandates should be imposed through a public regulatory process and be subject to annual recertification and assessment of their implications on cybersecurity and human rights.

7) Comprehensive Vulnerability Management. Governments must establish comprehensive vulnerability management that includes a transparent vulnerabilities equities process (VEP) to determine whether newly discovered and previously unknown software and hardware vulnerabilities should be disclosed or temporarily withheld for law enforcement purposes. The VEP should be enacted in law and subject to public reporting to the legislature and independent oversight.

8) Minimize Data Localization. Governments should minimize data localization requirements for law enforcement access. Targeted, sector-specific requirements may be permissible if other legal and regulatory tools cannot sufficiently guarantee lawful access.

9) Periodic Review. Any national encryption regime that enables lawful access to encrypted data in decrypted form must be maintained through a periodic review process. The process must allow for timely adjustments of different equities in a rapidly changing environment.

Proposed Regimes

EWI has constructed two proposed regimes which are generally consistent with the recommendations in this report.[3] The regimes reflect the outcome of an international, expert consultation aimed at identifying common ground, but not necessarily reaching consensus on encryption policy for lawful access. As a general matter, the experts considered both regimes as potentially effective and useful for law enforcement, if balanced by effective limitations to curb possible downsides in their application.

Both proposed regimes rely significantly on compelled provider assistance as a key policy approach to facilitate access to the plaintext of encrypted data. Law enforcement may legally require ICT service providers or manufacturers to provide assistance in decrypting information stored in or passing through their products, services or devices. This may include technical assistance to decrypt, intercept, manipulate and preserve data, or, to the extent permitted by law, to re-write firmware or software, or covertly install remote monitoring or control capabilities on specific devices. The law may set conditions including establishing judicial procedures, enhancing transparency and oversight, limiting the types of crimes covered, not requiring system modifications or providing reimbursement for costs incurred.

The titles of the two regimes, "Lawful Hacking" and "Design Mandates," are meant to highlight a key policy choice. Either

3 The proposed regimes are defined in Section 5.

Overview of Proposed Regimes	Regime 1: Lawful Hacking			Regime 2: Design Mandates		
	Data at rest		Data in transit	Data at rest		Data in transit
	Data stored in cloud	Data stored on end device	Communications	Data stored in cloud	Data stored on end device	Communications
Approaches						
Compelled Provider Assistance	●	●	●	●	●	●
Lawful Hacking	●	●	●	Does Not Apply		
Design Mandates	Does Not Apply			●	●	●
Systemic Improvements						
Capacity Building for Law Enforcement (LE)	**Applicable to All Regimes**					
Streamline the MLAT Process						
Enhance LE/Private Sector & International LE Cooperation						

approach would represent changes in current law and policy in most democracies, and each has upsides and downsides for all the various interests at stake. Further, the regimes need not be mutually exclusive. A nation could select elements from each, or decide that no change in the status quo is merited.

In addition to compelled provider assistance, Regime 1 employs lawful hacking as a critical component. Lawful hacking may exploit vulnerabilities in systems and devices, whether remote or local, or use social engineering to circumvent security protections. Law enforcement may deploy lawful hacking as a technique to gain access to a system to intercept communications, secure digital evidence or facilitate access to stored data or communications in plaintext.

In contrast, Regime 2 does not permit lawful hacking, relying instead on design mandates to secure access to plaintext. These mandates require that providers and manufacturers design, build and deploy products, services and devices with the capability to accommodate future lawful access requests. Mandates apply to end devices, cloud data and designated ephemeral messaging and encrypted messaging services.

Both proposed regimes are strengthened by systemic improvements that benefit law enforcement authorities' overall efforts to combat cyber-enabled crime and terrorism. They (a) invest in capacity building to improve the handling of various types of encrypted and unencrypted data; (b) streamline and reform the process, including Mutual Legal Assistance Treaty (MLAT) processes, for responding to requests for data stored outside the jurisdiction of the investigating agency; and (c) advance national and international cooperation among law enforcement authorities and the private sector (e.g., points of contacts for experts and specialists).

Encryption Policy in Democratic Regimes

Introduction

The EastWest Institute (EWI) has set out to identify and explore middle-ground proposals that acknowledge encryption's dual nature and that could feasibly be agreed upon and implemented on an international basis, at least among democratic governments.

Encryption is an essential tool for protecting digital data and communications. It supports privacy and other human rights, protects financial assets and proprietary data, enhances national security and thwarts cyber-enabled crime. Long used by banks and governments, its increasing use in business and by individuals is fueled by multiple developments, including the theft of business data and liabilities associated with data breaches, state surveillance of communication networks and the decisions of major ICT (information and communications technology) companies to provide strong, user-friendly encryption by default. However, the widespread use of encryption[4] reduces law enforcement's ability to access vital digital evidence and other critical information to fight crime. Some governments are responding to this "going dark" problem by considering restricting the availability or effectiveness of commercial encryption products and services. Opponents of such controls emphasize the substantial benefits of encryption and argue that the increasing connectivity and digitization of public and private life compensate for the loss of access and may herald the dawn of a "golden age of surveillance" for law enforcement.

EWI has set out to identify and explore middle-ground proposals that acknowledge encryption's dual nature and that could feasibly be agreed upon and implemented on an international basis, at least among democratic governments. By middle-ground proposals, we mean balanced, risk-informed, encryption policy regimes that would enable legally authorized law enforcement access to the plaintext of encrypted data in limited cases and within a clear legal framework embedding human rights safeguards. At the same time, they attempt to mitigate the risk that third parties could gain unauthorized access and breach the confidentiality of the encrypted data and communications.

The encryption debate often is oversimplified as a choice between "going dark"[5] and "keys under doormats,"[6] pitting law enforcement against the information technology industry and human rights advocates. The reality is more

4 In this report, we use the term "cryptography" to include several different cryptographic functions that increase information security, including enhancing authentication, enabling non-repudiation, preserving confidentiality and protecting information integrity. We use the word "encryption" to refer specifically to the confidentiality function, which may be implemented, for example, by locking a device or encrypting data.

5 "Going dark" is a term used by law enforcement and, in particular, the FBI to describe the situation in which law enforcement has the "legal authority to intercept and access communications and information pursuant to court order, but lacks the technical ability to do so." See, for example, remarks by FBI Director Christopher Wray on January 9, 2018 <https://www.lawfareblog.com/fbi-director-christopher-wrays-remarks-encryption-international-conference-cyber-security>; the speech by the former Director of the FBI, James Comey, at the Brookings Institution, Washington, D.C., October 2014 <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>; testimony of Valerie Caproni, former General Counsel of the FBI, "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies," before the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, United States House of Representatives, 112th Congress, 2011 <http://judiciary.house.gov/_files/hearings/printers/112th/112-59_64581.pdf>; the FBI's webpage on the "Going Dark problem" <https://www.fbi.gov/services/operational-technology/going-dark>; and IACP, Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence, 2015 <http://www.theiacp.org/portals/0/documents/pdfs/IACPSummitReportGoingDark.pdf>.

6 Harold Abelson and others, Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications (Boston, MA, 2015) <https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf>.

complicated,[7] and in fact, the various parties share many common interests. All stakeholders want to live in a safe and free society. As human beings, we want privacy and other human rights to be secure. We want law enforcement authorities to effectively prevent and solve crimes—in the physical and virtual space—within legal constraints. We want digital information to be secure from malicious actors. We want markets to reward innovation and function efficiently. The challenge before us is no less than managing the ways in which technological change affects those common interests. Technological innovation challenges the established order. Technology is transforming relationships among long-established institutions, including states and corporations. Technology is also shifting the relationships between those institutions and human society. The way such challenges are resolved is a testament to the underlying values of society.

With encryption, of course, there is no single society. No single nation can impose a monopoly on strong encryption technology. The genie is out of the bottle and taming it—to the extent possible and necessary—must be a collective effort. Governments and citizens must find a balance between human rights and the responsibility of the state to protect its citizens, including granting and safeguarding the freedom and security provided for in global declarations and states' constitutions.

The encryption debate is maturing. In 2018, the U.S. National Academies of Sciences, Engineering and Medicine will publish an important, comprehensive report that describes and offers a framework for analyzing the multiple interdependencies that must be considered in developing a national encryption policy.[8] EWI hopes our report will complement that work.

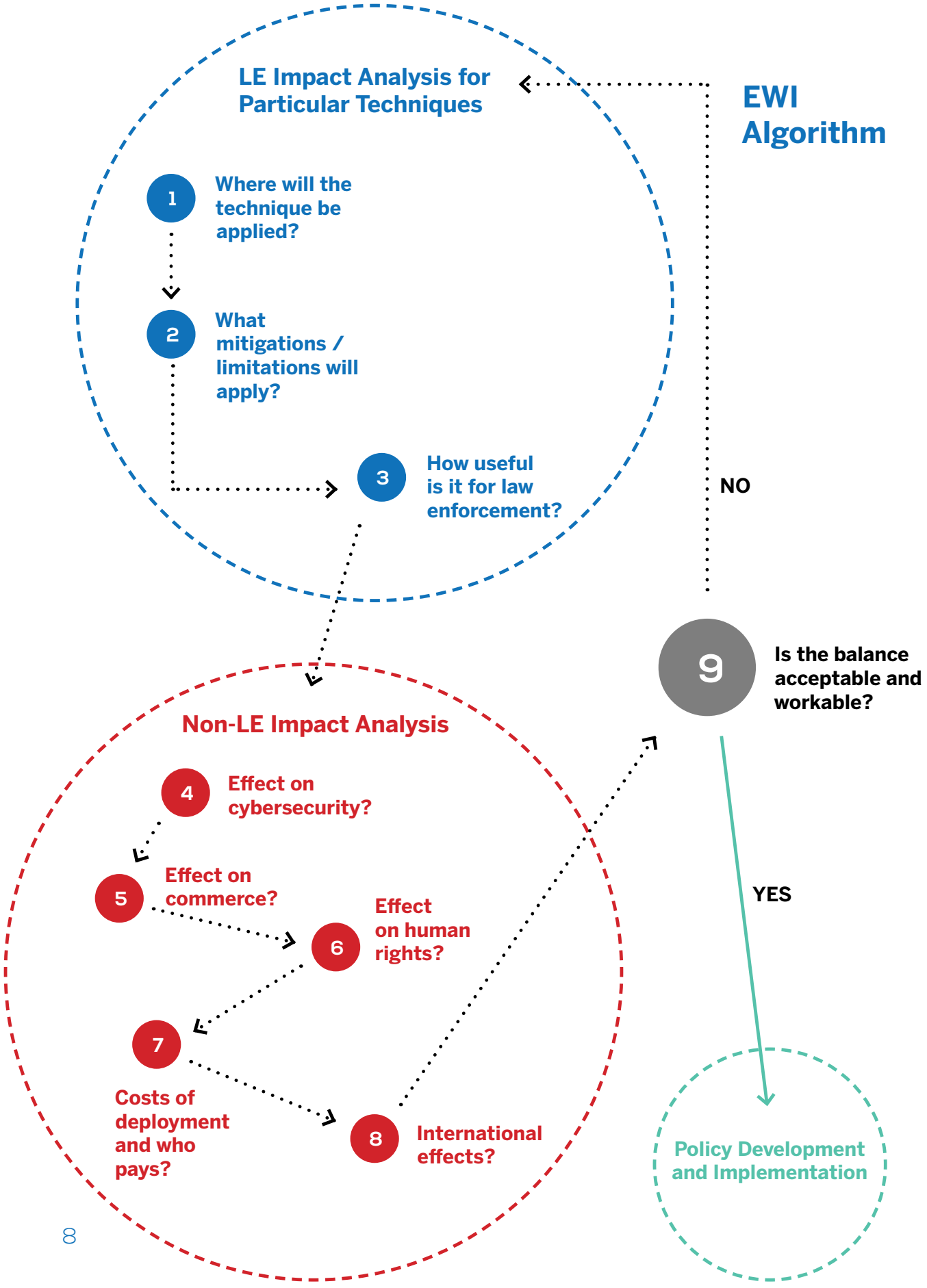
Structure of the Report

The remainder of this report contains six main sections:

- Section 2 postulates the need for balanced solutions, and frames common interests of the parties in terms of cybersecurity, law enforcement and public safety, commerce and privacy and other human rights. Principles and assumptions described in this section inform the path towards balanced solutions.
- Section 3 lays out key concerns important to each of those interests that continue to drive the encryption debate regarding lawful access to the plaintext of encrypted data.
- Section 4 introduces the EWI analytical framework: (a) three components that must be addressed in any encryption policy; (b) an algorithm that describes a way to evaluate the effects of policy choices (see figure on page 8); and (c) a process for applying the algorithm to produce one or more balanced encryption policy regimes. It also describes how EWI used the framework to develop the proposed regimes.
- Section 5 proposes two encryption policy regimes developed by EWI based on the work described in the previous two sections.
- Section 6 provides more general policy recommendations for policymakers and stakeholders.
- Section 7 concludes with thoughts on ways forward.

7 See for example the excellent "Don't Panic" report: Matt Olsen, Bruce Schneier, and Jonathan Zittrain, Don't Panic: Making Progress on the 'Going Dark' Debate (Boston, MA, 2016) <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf>.

8 National Academies of Sciences, Engineering, and Medicine, Decrypting the Encryption Debate: A Framework for Decision Makers (Washington, D.C.: National Academies Press, 2018) <www.nap.edu>.


LE Impact Analysis for Particular Techniques
1
Where will the technique be applied?
2
What mitigations / limitations will apply?
3
How useful is it for law enforcement?
EWI Algorithm
NO
9
Is the balance acceptable and workable?
YES
Non-LE Impact Analysis
4
Effect on cybersecurity?
5
Effect on commerce?
6
Effect on human rights?
7
Costs of deployment and who pays?
8
International effects?
Policy Development and Implementation

Conclusion

Encryption, a creature of cyberspace, is an international phenomenon. Collaboration on encryption policy across governments and companies is essential to protect privacy, fight crime and reduce compliance costs for global companies.

This report asserts that a balanced, transparent and risk-informed approach is necessary to find middle-ground solutions that acknowledge the competing interests and concerns that frame the debate about encryption policy for lawful access. It underscores the necessity of strong encryption while recognizing the challenges it creates for law enforcement and public safety.

The report advocates for policies that would better equip law enforcement to investigate and prevent serious crime and terrorism, while leaving in impediments to that capability in the interest of managing risk to other important societal interests. Rather than generally banning or weakening encryption, government must work more closely with the private sector. And the private sector, to reduce the risk of costly regulation, needs to understand and address law enforcement concerns. The targeted approaches to lawful access proposed in this report attempt to balance the "equities" of all the stakeholders.

First and foremost, the proposed regimes rely on transparency and the rule of law. While EWI does not advocate for any particular regime, we take here the privilege of the pen to express a preference. Design mandates are unattractive. No matter how carefully done, they risk undermining cybersecurity and all it protects. They will also generate unpredictable commercial consequences. But in our view, lawful hacking is the more dangerous choice. For no matter how much procedure, transparency and oversight is layered on, saddling police officers with the ambiguity and responsibility tied to using the deception, obfuscation and stealth that are part of modern hacking tradecraft risks creating unaccountable power that, as human history continues to show, is fraught with danger to the citizenry.

This report is meant as a constructive step in rationalizing the encryption debate. Innovation in technology and society will rapidly expose unknown unknowns that will no doubt soon make the report out-of-date. In addition, the report most certainly contains errors of fact and nuance. Encryption policy is complicated. Empirical data are missing. And, as Mr. Justice Holmes said, "Hard cases make bad law." We welcome comments from our readership. Please send them to cyber@eastwest.ngo.

Encryption, a creature of cyberspace, is an international phenomenon. Collaboration on encryption policy across governments and companies is essential to protect privacy, fight crime and reduce compliance costs for global companies. EWI will continue to work to enhance international cooperation on this important issue.

Acknowledgments

This report was prepared by the EastWest Institute and authored by **Andreas Kuehn** and **Bruce McConnell**. The authors are extremely grateful for the advice provided by the experts who have agreed to be listed here. Their inclusion here does not mean that they support or agree with any of the report's statements, proposals, recommendations or conclusions.

In particular, the report greatly benefited from the leadership, expertise and experience of the members of the EWI Breakthrough Group Ubiquitous Encryption and Lawful Government Access. The following experts participated in this Breakthrough Group:

Kamlesh Bajaj, Founder CEO, Data Security Council of India; Distinguished Fellow, EastWest Institute
Greg Brower, Assistant Director, Office of Congressional Affairs, Federal Bureau of Investigation
Scott Charney, Vice President, Security Policy, Microsoft Corporation
Jim Dempsey, Executive Director, Berkeley Center for Law & Technology, University of California, Berkeley
Udo Helmbrecht, Executive Director, European Union Agency for Network and Information Security (ENISA)
Kenn Kern, Chief of Staff to the Investigation Division, Special Assistant for International Relations, New York County District Attorney's Office
Tomas Lamanauskas, Group Director Public Policy, VEON
David R. O'Brien, Senior Researcher, Berkman Klein Center for Internet & Society, Harvard University
Stefan Schiffner, Postdoctoral Research Associate, SECAN-Lab, University of Luxembourg
Rodica Tirtea, Expert in Network and Information Security, European Union Agency for Network and Information Security (ENISA)

The following experts provided substantive commentary and advice during the development of this report:

Michael Chertoff, Executive Chairman and Co-Founder, The Chertoff Group; Former U.S. Secretary of Homeland Security; Member, Board of Directors, EastWest Institute
J. Michael Daniel, President and CEO, Cyber Threat Alliance
Jon Eisenberg, Senior Director, Computer Science and Telecommunications Board, National Academies of Sciences, Engineering, and Medicine
Sven Herpig, Project Director, Transatlantic Cyber Forum, Stiftung Neue Verantwortung e.V.
Herb Lin, Senior Researcher Scholar for Cyber Policy and Security, Center for International Security and Cooperation, Stanford University
Riana Pfefferkorn, Cryptography Fellow, Stanford Center for Internet and Society
Lodewijk van Zwieten, Public Prosecutor, The Netherlands

As noted in Section 4.4, some 30 experts participated in an early informal workshop discussion on this topic, providing valuable direction and insights.

The following EWI associates provided invaluable support and assistance for this report: **Michael Depp**, **Conrad Jarzebowski**, **Ethan Kim**, **Abagail Lawson**, **Anneleen Roggeman**, **Alex Schulman**, **Spandana Singh** and **Dragan Stojanovski**.

Global Cooperation in Cyberspace Initiative

SUPPORTERS:

Microsoft
Huawei Technologies
Unisys
Sonus Networks
Qihoo 360
NXP Semiconductors
CenturyLink
VEON
JPMorgan Chase
Marsh & McLennan
The Hague Centre for Strategic Studies
William and Flora Hewlett Foundation

PARTNERS:

IEEE Communications Society
Munich Security Conference
The Open Group
Fudan University
University of New South Wales
Center for Long-Term Cybersecurity, University of California, Berkeley

Read the full report at **eastwest.ngo/encryption**

Encryption Policy in Democratic Regimes
Finding Convergent Paths and Balanced Solutions

EastWest INSTITUTE

New York | Brussels | Moscow | San Francisco
www.eastwest.ngo | **t:** @EWInstitute | **f:** EastWestInstitute