EastWest INSTITUTE

Encryption Policy in Democratic Regimes

Finding Convergent Paths and Balanced Solutions

ISBN 978-0-9856824-6-0

The views expressed in this publication do not necessarily reflect the position of the EastWest Institute, its Board of Directors or staff.

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.

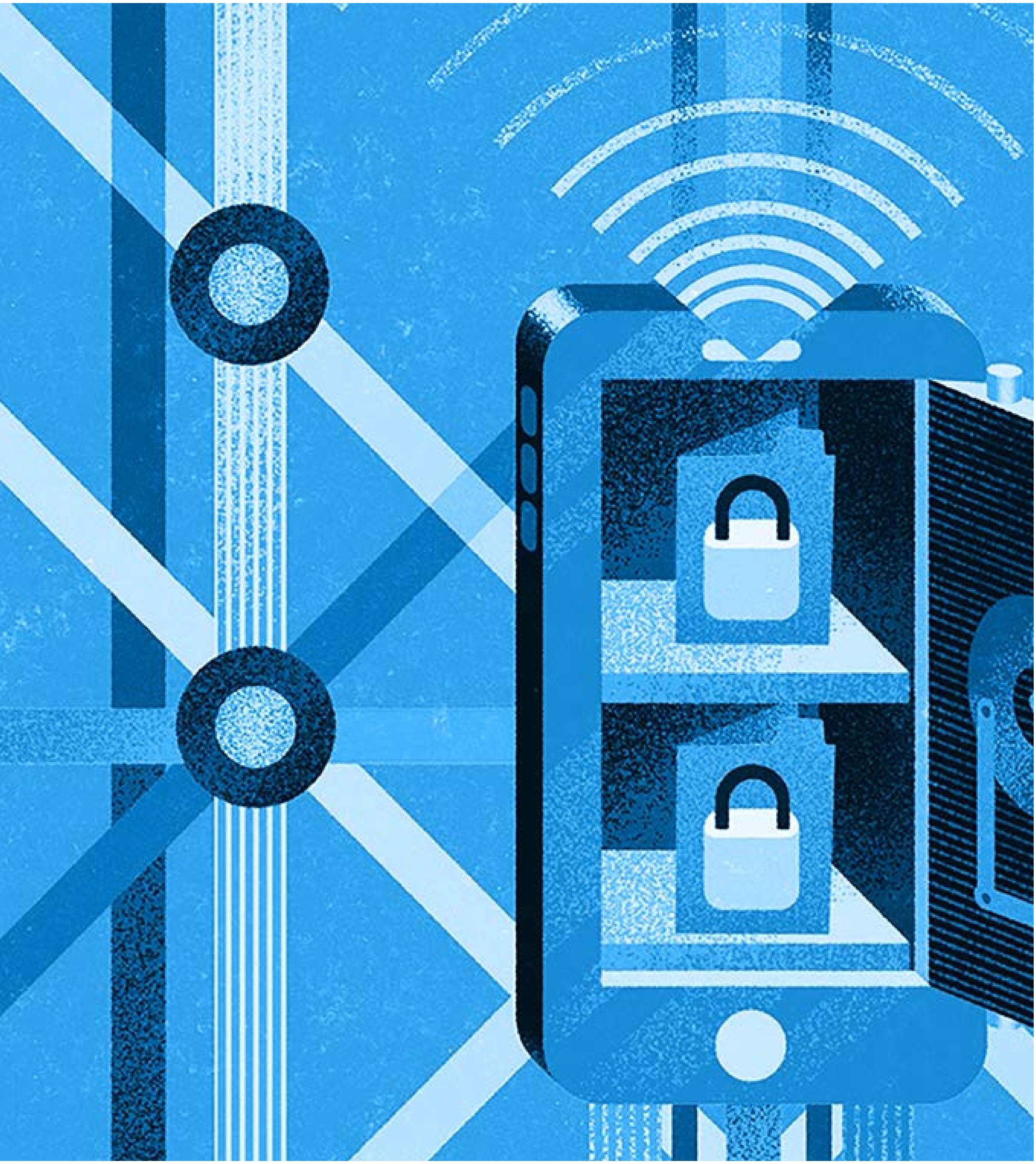
Recommendations

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

[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.



promote strong cybersecurity. Governments must refrain 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

[3] The proposed regimes are defined in Section 5.

	Regime 1: Lawful Hacking			Regime 2: Design Mandates		
	Data at rest		Data in transit	Data at rest		Data in transit
Overview of Proposed Regimes	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						

Mandates," are meant to highlight a key policy choice. Either 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

1 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

[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>.

human rights advocates. The reality is more 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.

1.1 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; 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>.

2 The Need for Balanced Regimes

This report views the encryption debate as a set of competing, but largely common, interests. All people want security, but we may disagree as to which elements of security a society should emphasize.

This report argues that a variety of middle-grounds should be explored, notwithstanding the polarization evident in the public conversation, because very few societies will find it acceptable to emphasize one kind of security to the exclusion of another. Therefore, finding effective, principled regimes is important to avoid arriving at a one-sided approach driven by crisis and fear.

This report proposes encryption policy solutions for law enforcement access that take into account the perspectives, needs and interests of different stakeholders. The proposed encryption policy regimes are meant to provide law enforcement some access to the plaintext of encrypted data, and do so in a way that protects other interests including cybersecurity, commerce, and privacy and other human rights. This approach has implications for both the outcomes (e.g., plaintext may not always be available) and the process (e.g., there must be transparency and adherence to the rule of law). Balancing multiple interests requires tough trade-offs. As with any compromise, no party will achieve all its goals.

2.1 Common Interests Frame the Debate

One can evaluate any government encryption policy on its effects; policies reflect the values and priorities of the various stakeholders. We have identified four such value sets that interact with each other:

1. Cybersecurity: This value set emphasizes the importance of ensuring that digital information is kept secure, focusing on its confidentiality, integrity and availability. Policies favorable to this value set increase users' trust that their transactions and data are secure and safe. Undermining that trust in information and communications technology (ICT) and the Internet could lead users to abandon some digital services and technologies, creating social, political and economic dislocations. Proponents argue there is a need for strong, ubiquitous encryption to protect critical data and infrastructure in the private sector, government and among citizens. Encryption is a critical and effective safeguard against the theft of data, malicious data manipulation, and cyber espionage, as well as for the protection of privacy and other human rights.

2. Law Enforcement and Public Safety: This value set emphasizes the importance of ensuring that, within legal constraints, law enforcement can access digital evidence and information to prevent, solve and prosecute crimes.[9] It emphasizes the need for law enforcement entities to possess

[9] While it is common in an Anglo-Saxon context to define law enforcement as the combination of the police and the prosecution service, in countries where the prosecution service is part of the magistracy, it can be confusing to capture them under the term "law enforcement." For the purposes of this report, however, we have used "law enforcement" to cover all elements of the system. More importantly, as we recognize elsewhere, there are distinctions across democracies in authorities of the various services, with impacts on their independence from each other.

the technical ability and means to access the data they need, subject to their obtaining the necessary legal justification to access this data in accordance with due process of law. Law enforcement, as a guarantor of public safety, also has an interest in cybersecurity to reduce the incidence of cyber-enabled crime.

3. Commerce: This value set focuses on market-led policies that reward innovation and efficiency. Such policies enhance or enable a free market for encryption products and services, without limitation of features, country of origin and so forth. In general, market-led policies have favored the continued development of stronger and more user-friendly encryption that is widely available (i.e., ubiquitous encryption). Moreover, where specific features are required, innovators will seek to find ways to satisfy them.

4. Privacy and Other Human Rights: This value set emphasizes policies designed to protect privacy and other human rights, including the right to live in a safe and free society. These have generally been couched as supporting the need to have strong encryption to protect citizens and dissidents from state power, particularly those in authoritarian regimes. Encryption is a tool to protect human rights, such as the rights to privacy and freedom of opinion and expression.

These value sets interact in ambiguous and subtle ways, and while societies differ in the relative value they place on each one, no society can emphasize one to the exclusion of all others. Further, the value sets do not always neatly line up with either of the two traditional poles of the argument (i.e., privacy/security vs. national security/public safety). For example, policies supporting the use of strong encryption for cybersecurity purposes can benefit law enforcement's ability to protect citizens by preventing cyber-enabled crime. On the other hand, policies enabling law enforcement access can benefit citizens by upholding public safety in the course of preventing crime or terrorism. These contradictions are discussed further in Section 3, "Concerns."

2.2 Principles and Assumptions Informing Balanced Regimes

In order to achieve a balanced regime, EWI identified a set of key principles and assumptions that guide the issue analysis and the development of encryption policy regimes. We define the concepts as follows:

- Principles: Principles reflect the values that guide the judgments arrived at in the report. They are not absolute statements, but reflect desired preferences. In some cases, not all principles are achievable at the same time.
- Assumptions: Assumptions describe underlying beliefs about realities, hypotheses, predictions and conditions. Making them explicit creates the opportunity to discuss, challenge and test these assumptions as part of the ongoing development of possible balanced regimes. Assumptions may sometimes conflict with each other, based on differing viewpoints and conceptualizations. These differences need to be taken into account when crafting regimes.

2.2.1 Principles

1. Balance Principle: It is important to find balanced solutions to the encryption challenge in the digital world that account for the interests and equities of the various stakeholders. For example, this principle recognizes the complex trade-offs between individual privacy, business information security and public safety. Public safety, like individual privacy, is a human right.

2. Do-No-Harm Principle: Consistent with the Balance Principle, solutions should minimize adverse effects and unintended consequences to the extent practicable.

3. Proportionality Principle: Where adverse effects are unavoidable, the relative proportion to anticipated gains should be considered. Acceptable proportions may vary by case. For example, in a situation where lives are at stake, a higher proportion of infringement on human rights may be tolerated for gains in security.

4. Transparency Principle: Solutions that provide for transparency about decryption and information access capabilities, about requests from and responses to law enforcement needing access to decrypted information and notification of targets will increase accountability and public trust.

5. Holistic Approach Principle: Governmental concerns with lawful access are not limited to encryption. Likewise, the "solution" will likely consist of different elements that are difficult to align with each other. The costs of "doing nothing" should also be considered.

6. Forbearance Principle: Moving forward with new technologies and approaches to data collection and analysis, not everything that is technologically possible should become an acceptable tool for law enforcement. A meaningful debate needs to take place about acceptable, balanced limits and standards.

7. Culture Principle: Differing cultural values and existing laws will affect where the balance is set on these issues in a given society. The potential for these differences, even among democracies, should be taken into account.

2.2.2 Assumptions

1. No single solution will solve all problems. Different solutions for different democratic regimes will emerge, depending on their specific institutional and cultural settings and requirements.

2. Even if governments do not enact policy, law enforcement will continue to innovate and seek access to plaintext, using all tools legally at their disposal.

3. Democratic regimes can devise overall effective encryption policies that reduce the risk of abuse and exploitation while providing access to law enforcement, in some cases. However, no risk-free or costless solutions exist. All approaches impose some cost to society, either through the risk to public safety (e.g., law enforcement cannot access the data it needs) or to cybersecurity or human rights (e.g., limitations on encryption to grant lawful access). Particularly in democracies, trade-offs will occur (e.g., there will be no absolute right to privacy nor absolute access for law enforcement).

4. Human rights cannot be protected if law enforcement is ineffective. And, limits on law enforcement's authorities and activities are an essential part of a meaningful human rights regime.

5. Encryption is a serious practical barrier to law enforcement's ability to prevent and investigate crimes.

6. The role of encryption in protecting data and communications will increase given societies' growing dependence on ICT and the growing availability of encryption technology.

7. With the Internet of Things and other new areas of use, ever-increasing flows of data become available as potential sources for law enforcement. However, access to plaintext will remain essential in certain circumstances.

8. Encryption is not the only barrier. Data may be in undocumented or otherwise unfamiliar formats, out of reach (e.g., in a different jurisdiction) or ephemeral.

9. Any technical means that provide lawful access to plaintext increases the risk that criminals will exploit these means and maliciously use that access to commit crime.

10. In the arena of security, ICT product and service providers should be treated more like telecommunications companies than traditional manufacturers. While we do not require safe manufacturers to retain the ability to access safes that they have made, law enforcement has readily available, effective alternatives to access information protected by a safe or a physical lock. The ubiquity and criticality of ICT products and services to modern life suggests that providers hold a different position in the marketplace, and governmental policies should reflect this difference.

11. Giving law enforcement unrestricted lawful access may lead to abuse. Law enforcement must recognize societal mistrust regarding its ability to access data (e.g., does law enforcement follow the law, abuse power, ask for more capabilities than it needs, have more capabilities than it admits, work secretly with intelligence agencies to break encryption and so forth).

12. National encryption policies have international ramifications. Providing capabilities to national law enforcement will trigger foreign requests to provide data; some requests may come from countries with lower legal standards. This is particularly relevant to the protection of human rights in authoritarian regimes.

3 Concerns

This section lays out key concerns that stem from four value sets, and that have been influential and continue to drive the encryption debate regarding lawful access to the plaintext of encrypted data.

In Section 2 we laid out four areas of common interest and corresponding value sets—cybersecurity, law enforcement and public safety, commerce and privacy and other human rights—shared by many people. This section lays out key concerns that stem from those value sets, and that have been influential and continue to drive the encryption debate regarding lawful access to the plaintext of encrypted data.

3.1 Cybersecurity

Encryption is essential to cybersecurity as it provides confidentiality to data and communications to protect against unwanted disclosure. All domains of society rely on encryption to securely use ICT services and products, for instance, securing money transfers on global financial transaction networks or sharing sensitive information on public networks.

Encryption is based on cryptographic functions that provide confidentiality, also affording authentication, non-repudiation and integrity.[10] To encrypt or decrypt data, an encryption algorithm is used together with a key. The key is a mathematical concept and in most cases, users employ one or multiple factors (e.g., a password, passphrase, or biometric fingerprint) to unlock the lengthy cryptographic key, which, together with the encryption algorithm, encodes plaintext into scrambled, non-readable ciphertext. In a well-designed encryption system, the key or password is solely accessible to the user and not to third parties. As such, only a particular user has the ability to decrypt and read the data in plaintext that was previously encrypted with a particular key. In practice, less strict requirements may apply; for instance, a system might have implemented a key recovery mechanism for business continuity purposes to regain access should the password (and with it, the key) have been lost or forgotten.

Cryptographic products and services for all types of data and communications are widely available. Encryption is used to protect stored data of various types, ranging from individual files, to partitions or the entire storage system.[11] Some instances employ a combination of software and hardware to encrypt data securely (e.g., trusted platform module (TPM), and hardware security module (HSM) microcontrollers). To secure communications, in recent years, a wide range of secure messaging apps that offer end-to-end encryption have become widely available and popular.[12] To secure Internet traffic, the Transport Layer Security (TLS) protocol is used (e.g., HTTPS) and Virtual Private Networks (VPN) provide traffic encryption through a virtual tunneling protocol. Security and privacy-conscious email service providers offer email encryption.[13] Other means to protect privacy and anonymity online come in the form of ephemeral communication and anonymization services. Ephemeral messaging services delete messages after a few seconds[14] and anonymization services re-route and re-encrypt Internet traffic to obscure the initial requesting IP address.[15]

[10] OWASP, 'Guide to Cryptography' <https://www.owasp.org/index.php/Guide_to_Cryptography#Cryptographic_Functions>.

[11] Examples include BitLocker, TrueCrypt, VeraCrypt, and 7-Zip.

[12] Examples include Facebook's WhatsApp, Apple's iMessage, and Signal.

[13] Examples include ProtonMail and riseup.net.

[14] Examples include SnapChat and Wickr.

[15] Examples include Tor (The Onion Routing Project) and I2P (Invisible Internet Project).

Technology experts have repeatedly pointed out the importance of encryption for cybersecurity and other subsequent areas of security that rely heavily on cybersecurity, including national security and the financial services sector. Undermining encryption, these experts argue, will introduce significant risk and have detrimental effects on cybersecurity.[16] Strong encryption is also supported by various international and governmental bodies. For instance, the European Union confirmed that "strong and trusted encryption is highly important for properly ensuring human rights and fundamental freedoms," while recognizing the impediments law enforcement authorities are facing as a result of strong encryption and anonymization technologies.[17] Also, the United Nations[18] and the Netherlands[19] have issued statements in support of encryption and against restrictive measures that undermine the protections encryption confers. In the U.S., the Encryption Working Group of the House Judiciary Committee and the House Energy and Commerce Committee concluded that "any measure that weakens encryption works against the national interest."[20]

3.2 Law Enforcement and Public Safety

While encryption products and services briefly described in the previous section are most often used for legitimate purposes to protect data and communications, criminals and terrorists have been using the same tools to obfuscate their malicious activities. Major ICT and Internet service providers have stepped up their security in recent years to provide their users some encrypted services and products by default. While the Snowden disclosures have been an important driving factor in this development, the increase in cyber crime and cyber espionage, coupled with policy developments that made corporations accountable for the proper protection of customer data (e.g., liability for data breaches and loss of customer data), has further increased the need for encryption. Some companies have deliberately made design decisions that make it impossible for them to provide effective technical assistance. Law enforcement is confronted with situations in which devices are lawfully seized but remain inaccessible due to encryption—losing vital access to data for crime and terrorism detection, prevention, investigations and prosecution. For instance, the Manhattan District Attorney's Office reported that over 700 of the devices it seized in 2017 came locked using full-disc encryption, and the FBI has said it was unable to access data on 7,000 encrypted devices in the same year.[21] Encryption has certainly become a challenge for law enforcement, as it has become widely available through smart phones and messaging apps that provide encryption by default and designed to make the decryption key solely available to the particular user. It is likely that crime and terrorism will increasingly deploy encryption for online and offline activities in some form (e.g., low- and high-level crimes, including communications with a drug dealer through a messaging app or white collar crimes, such as government corruption or insider trading). Encryption as a barrier for law enforcement is found in cases ranging from financial crime, murder, child pornography, drug offenses, terrorism and copyright violation, to espionage, computer crime and kidnapping.[22]

[16] Abelson and others.

[17] Council of the European Union, 'Council Conclusions of 20 November 2017 on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU', 2017 <http://www.consilium.europa.eu/media/31666/st14435en17.pdf>; and European Commission, '2017 Eleventh Progress Report towards an Effective and Genuine Security Union', 2017 <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf>.

[18] UN Office of the High Commissioner, 'Report on Encryption, Anonymity, and the Human Rights Framework', 2017 <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>.

[19] ENISA, 'The Netherlands: Cabinet Launched Position on Encryption', ENISA, 21 April 2016 <https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/the-netherlands-cabinet-launched-position-on-encryption>; Dutch Ministry of Security and Justice, Cabinet's View on Encryption, 2016 <https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on-encryption>.

[20] U.S. House Judiciary Committee and the House Energy and Commerce Committee, 'Encryption Working Group Year-End Report' (Washington, D.C.: Encryption Working Group, 2016) <https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf>.

[21] New York County District Attorney, Smartphone Encryption and Public Safety (New York, NY, 2017), p. 5 <http://manhattanda.org/sites/default/files/2017 Report of the Manhattan District Attorney's Office on Smartphone Encryption.pdf>.

[22] For a collection of cases, see, http://scienceblogs.de/klausis-krypto-kolumne/when-encryption-baffles-the-police-a-collection-of-cases/.

While access to plaintext can provide important data and evidence, in numerous cases, suspects eventually were convicted without law enforcement gaining access to decrypted data in plaintext, indicating that access to decrypted data is not always necessary for prosecution. Inaccessibility of encrypted data has further downsides, including that other crimes committed by the suspect may not be discovered, some victims may be harder to identify and protect, some coconspirators may be impossible to identify and arrest, and some sentences will not reflect the full scope of the defendant's criminal conduct. For preventive measures, including counterterrorism, lack of access may be more problematic in cases where digital content (e.g., plans) is critical to preventing serious incidents.

Investigations involving digital evidence are complex endeavors that go beyond the question of access to a single encrypted device; they may include sophisticated practices and technologies to evade the authorities, creating additional challenges when an investigation covers multiple jurisdictions.[23] Organized crime often deploys complex technical infrastructures and uses multiple levels of encryption (e.g., using readily available encrypted SSL/TLS channels, widely used by all Internet users to protect Internet traffic).[24]

Cyber crime and terrorism operations increasingly are carried out from multiple jurisdictions. Consequently, authorities increasingly are confronted with cross-border issues and face further challenges when requesting lawful access to data stored or transmitted in foreign jurisdictions or controlled by persons falling under foreign jurisdictions. While not specific to encrypted data, cross-border requests for evidence or data sharing are increasingly common in all kinds of criminal investigations. Organized crime structures its activities knowingly to evade law enforcement authorities constrained to a single jurisdiction. In addition, services and data increasingly are provided and stored in the cloud, with cloud service providers (including both public and private clouds) often operating their physical server farms in multiple jurisdictions. These trans-border issues go well beyond where the data is stored. Forthcoming European regulations attempt to deal with this quandary by taking an expansive approach to jurisdiction, encompassing the provider, data or data subject. This will further complicate compliance with law enforcement assistance requests between EU and non-EU law enforcement authorities.

For cross-border cooperation in law enforcement investigations, Mutual Legal Assistance Treaty (MLAT) processes serve as established channels to share requested information. However, MLAT procedures are complex, slow and cumbersome. Most jurisdictions lack sufficiently trained personnel to process the increasing number of requests from foreign law enforcement authorities. Calls for modernizing the MLAT process continue.[25] The U.S. Congress has drafted legislation that would allow bilateral agreements with other partners, such as the UK, that under certain conditions, a foreign law enforcement authority can directly request and serve a foreign lawful access request (e.g., warrant) on a domestic company.

3.3 Commerce

Commercial interests are reflected in concerns about the potential disruptive effects of encryption policy on the ICT market in terms of administrative burden and compliance costs, firms' ability to innovate and remain competitive in the global ICT market, and the ability of business to conduct digital commerce securely. Encryption is a key security mechanism to protect transactions, communications and stored data from unauthorized access or harmful leaks. The financial services industry, for instance, depends on encryption to protect credit card transactions and secure online banking, and to safeguard sensitive consumer data stored in the banks' applications and databases.

Today, there is a healthy ecosystem of developers and vendors in at least 36 countries that provide a variety of encryption products and services. A 2016 global survey counted 805 encryption products in 35 different categories.[26] The largest product categories (with more than 50 percent or 424 products) consisted of message, mail and file encryption, and VPN solutions. The wide availability of commercial and open source encryption products and services makes effective government control quite difficult. Mobile device manufacturers and mobile operating system providers, in particular, have contributed significantly to the spread of by-default, ubiquitous encryption. Indeed, some ICT firms market their products and services as privacy-preserving technologies that will prevent unauthorized parties from getting access to data stored on these devices. Using sophisticated hardware and software protections, access to Apple and some Android mobile devices has become more difficult, even for authorities lawfully authorized to obtain access.[27]

The private sector continues to push back when governments propose to regulate encryption. For one, the ICT

[23] One expert noted that the technical analysis of a high-profile case lasted less than two weeks, but that it took the authorities two years to locate and arrest a criminal who operated from multiple jurisdictions.

[24] Group-IB, Lazarus Arisen: Architecture, Techniques and Attribution, 2017 <https://www.group-ib.com/resources/threat-research/lazarus.html>.

[25] Andrew Woods, Data Beyond Borders: Mutual Legal Assistance in the Internet Age, 2015 <https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf>.

[26] Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar, 'A Worldwide Survey of Encryption Products', 2016 <https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf>.

[27] Apple turned on full-device encryption by default in iOS 8 (2014), and Google followed and turned on full-device encryption by default in Android 6.0 Marshmallow (2015).

industry fears that such regulation would have significant negative effects for cybersecurity, and would impose significant compliance costs and lead to loss of market share against technologies from other nations that do not impose similar regulations. The Organisation for Economic Co-operation and Development (OECD), for instance, called on governments to avoid cryptography policies that create unjustified obstacles to trade, the flow of encrypted communications and the availability of cryptographic methods.[28] Differing national regimes (which may likely involve contradictory legal and data privacy protections) can increase product costs and create legal jeopardy, including forcing companies to decide which nation's laws to abide by.

3.4 Privacy and Other Human Rights

Encryption is essential to an individual's exercise of human rights, in particular, the rights to privacy, freedom of opinion and expression and other fundamental human rights.[29] International declarations and treaties ensure these rights. The right to privacy as a human right is established in Article 12 of the Universal Declaration of Human Rights (UDHR)[30] and enshrined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[31] In this context, privacy of communications is an important aspect of the right to privacy.[32] To this end, UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, stated:

> "In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous. Privacy of communications infers that individuals are able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State itself."[33]

Similarly, the right to freedom of opinion and expression is rooted in Article 19 of the UDHR[34] and enshrined in Article 19 of the ICCPR.[35] While varying in scope, similar language applicable to electronic communications is reflected in other human rights regimes, as well. The right to freedom of opinion and expression are "indispensable conditions for the full development of the person" and "essential for any society;"[36] even more, states have a positive obligation to protect citizens against infringement on their right to freedom of expression.[37] La Rue's successor, David Kaye, noted:

> "Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks."[38]

Encryption enables individuals to access and share content that would be otherwise inaccessible due to censorship, filtering and blocking. Kaye concluded that, "encryption

[28] OECD, Recommendation of the Council Concerning Guidelines for Cryptography Policy, 1997 <http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=115&InstrumentPID=111&Lang=en&Book=False>.

[29] Other human rights include freedom of association, peaceful assembly, and freedom of religion, as well as the rights of the victim. For the latter, see, Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA < http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2012:315:TOC>.

[30] Article 12, UDHR: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

[31] Article 17, ICCPR: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

[32] Wolfgang Schulz and Joris van Hoboken, 'Human Rights and Encryption', UNESCO Series on Internet Freedom, 2016, p. 54 <http://unesdoc.unesco.org/images/0024/002465/246527E.pdf>.

[33] Frank La Rue, 'UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', United Nations Human Rights Council, 2013 <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>.

[34] Article 19, UDHR: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

[35] Article 19, ICCPR: "1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals."

[36] UN Human Rights Committee, 'UN Human Rights Committee, General Comment on Freedom of Opinion and Expression', CCPR/C/GC/34, 2011, para. 2 <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

[37] UN Human Rights Committee, para. 11.

[38] David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Human Rights Council, A/HRC/29/32, 22 May 2015, p. 7. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf>.

0100100
1011011
0100100
1011011

and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection."[39] In addition, constitutional courts, such as the U.S. Supreme Court, the German Bundesverfassungsgericht and the European Court of Human Rights, have recognized unhindered communications—enabled by encryption—as an essential precondition for freedom of communication.[40]

Individuals should be able to communicate without fear of surveillance or observation, which otherwise would change the nature of communication and distort the rights to privacy and freedom of opinion and expression. Encryption ensures the confidentially of private communication. Even if intercepted, the communication cannot be read or altered. Encryption is also effective against mass surveillance. This holds particularly true for citizens in states in which these fundamental rights are not upheld by the rule of law or are not enjoyed by political oppositions and minorities.[41]

Yet, human rights are not absolute. As governments have an obligation to fight terrorism and crime, limitations to human rights for national security and public order exist to balance human rights to privacy and freedom of opinion and expression against the interests of public safety.[42] Restrictions, however, must comply with strict criteria set forth in the international human rights framework.[43] In the 2015 ruling Schrems v. Data Protection Commissioner of Ireland, the Court of Justice of the European Union decided that "legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life."[44]

With the advent of new approaches and technical tools, including monitoring capabilities that law enforcement authorities may acquire, the international human rights framework and legal safeguards must strive to keep pace. The 2013 report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, which addressed new means and modalities of communication surveillance, described lawful hacking and surveillance capabilities that exploit security vulnerabilities as "extra-legal surveillance" and "extremely disturbing."[45] Such capabilities pose a significant risk to human rights as they are "virtually undetectable" and allow a state to exercise full control over a device, including intercepting and modifying communications, commandeering the device's microphone or camera or modifying data on the device.[46] Such technologies—and their sale and transfer to authoritarian regimes—were heavily criticized as it became known in the aftermath of the Arab Spring that Western technology firms sold these surveillance capabilities to regimes with questionable human rights records. Consequently, the U.S. banned sales of surveillance technologies to Iran and Syria[47] and surveillance technologies were added to the control list of the Wassenaar Arrangement,[48] a multilateral export control regime. Some have argued that, with the private sector playing a central role in enabling states to conduct surveillance, including providing monitoring and decryption capabilities for law enforcement, states have a responsibility to hold corporations accountable for human rights violations as a result of their business conduct.[49]

In the encryption debate, human rights sometimes are treated as a secondary matter, taking a backseat to other important issues, such as national security and economic interests. Human rights advocates argue that it is essential to enhance the role that human rights play in these debates to preserve fundamental rights in the digital age.[50]

[39] Kaye, p. 1.

[40] Schulz and van Hoboken, p. 54.

[41] Freedom House, 'Freedom House's Annual Freedom in the World and Freedom on the Net Reports on the Global Development of Political, Civil, and Digital Rights', Freedom on the Net 2017, 2017 <https://freedomhouse.org/reports>.

[42] The 2011 report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression expressed concerns about nation states' actions against and justification for the interference with individuals' online communications on the grounds of protecting national security and fighting terrorism. See, Frank La Rue, 'The 2011 Report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,' Human Rights Council, 2011, p. 15 <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>.

[43] For a legal framework to evaluate restrictions on encryption, see, Kaye.

[44] Court of Justice of the European Union, Judgement of the Court (Grand Chamber), 6 October 2015, para. 94 <http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=116845>.

[45] La Rue, 'UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression', para. 16. (A/HRC/23/40).

[46] La Rue, 'UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', para. 11. (A/HRC/23/40).

[47] The White House, Executive Order -- Blocking the Property and Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology, The White House Archives, 2012 <https://obamawhitehouse.archives.gov/the-press-office/2012/04/23/executive-order-blocking-property-and-suspending-entry-united-states-cer>.

[48] The Wassenaar Arrangement is a multilateral export control regime for conventional arms and dual-use goods and technologies. See, http://www.wassenaar.org/

[49] La Rue, 'UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression', para. 20. (A/HRC/23/40).

[50] Schulz and van Hoboken, pp. 60–61.

4 EWI Analytical Framework

We describe a set of (1) techniques and (2) limitations that are applicable to (3) a particular ICT environment.

EWI's approach to fostering dialogue among interested parties to help develop balanced encryption policies begins with an analytical framework that includes three components (Section 4.1) that must be addressed in any encryption policy, including:

- What techniques are permitted (e.g., government hacking);
- What limitations on the use of these techniques are in place (e.g., authorization via court order); and
- Where in the ICT environment the technique is permissible (e.g., data stored on end devices such as smart phones).

The framework also includes an algorithm (Section 4.2) that describes a way to evaluate the effects of policy choices and the extent to which a policy is "acceptable" and "workable" from various perspectives. The algorithm assists in balancing across differing equities by making explicit the various interests and needs of the stakeholders.

Finally the framework includes a process (Section 4.3) for applying the algorithm to produce one or more encryption policy regimes that would enable law enforcement access or otherwise compensate for the consequences of limited or denied lawful access.

4.1 Three Components that Must Be Addressed in Any Encryption Policy

- **Techniques:** These describe approaches that allow law enforcement to directly or indirectly access encrypted data in plaintext (or other relevant data in an investigation) or to deny or restrict the effective use of encryption technology.
- **Limitations:** These describe a set of conditions that constrain the use, effectiveness or efficiency of the techniques in favor of other interests (i.e., cybersecurity, commerce and human rights).
- **ICT Environment:** This describes the ICT infrastructure where targeted data is extracted. This report differentiates between "data at rest" and "data in transit" and looks at the following three categories: (1) cloud (data at rest); (2) end device (data at rest in a mobile phone, desktop computer, etc.) and (3) analog and digital voice and data communications (data in transit).

The three key components span a 3-D space, as depicted in Figure 1, that can encompass numerous policy options: Techniques, Limitations and the ICT Environment.

In the process of selecting and adopting encryption policies for a particular setting, we describe a set of (1) techniques and (2) limitations that are applicable to (3) a particular ICT environment. These sets are referred to as a "policy option" or "technique use policy." Any set of relevant options that make an overall balanced approach to the plaintext access problem is referred to as an "encryption policy regime." Ideally, an encryption policy regime reflects an understanding of the entire ICT environment, while limiting its application to the most critical areas.

4.1.1 Techniques for Law Enforcement Access to Plaintext of Encrypted Data

Techniques describe policy and/or technical approaches to gain access to the plaintext of encrypted data or prevent the use of effective encryption technologies. Governments have technical and legal means at their disposal to reduce the potential impact of encryption on law enforcement.

Table 1 provides an overview of the techniques discussed here. A legal framework (generally at the national level) will prescribe how a law enforcement agency can deploy any particular method, and what legal and procedural requirements must be satisfied to constitute lawful deployment. Some methods come with broad implications and affect a wide spectrum of users, while others are targeted narrowly to a particular product, service or even an individual user. Each method creates specific security and risk

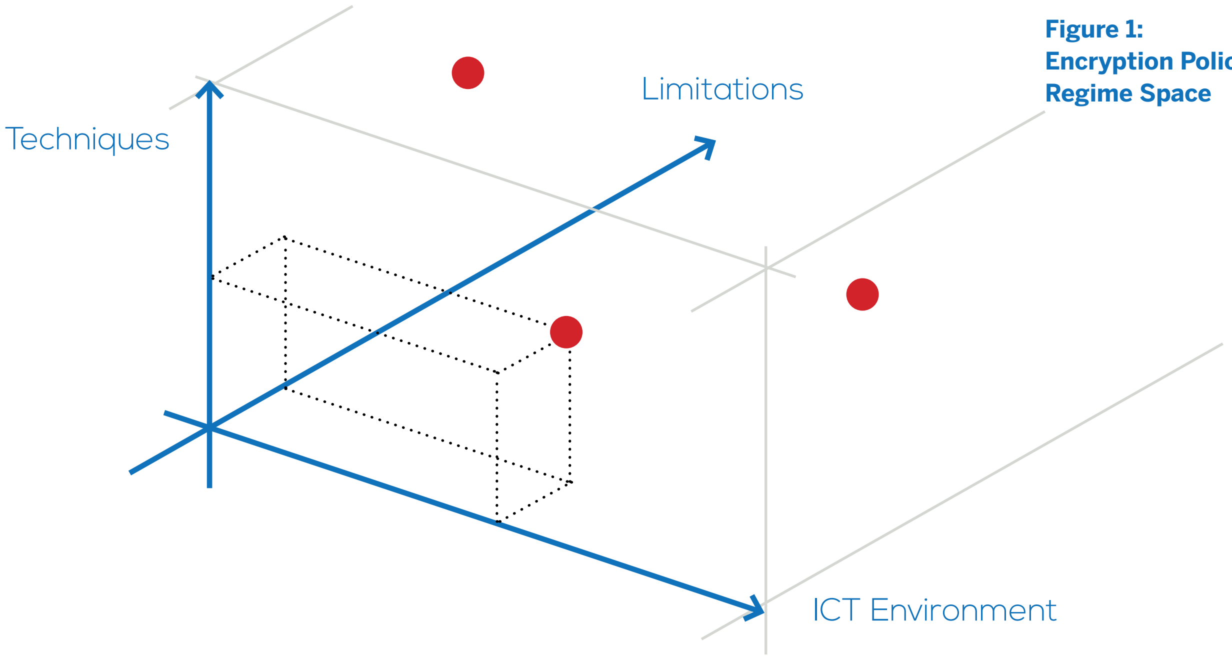


Figure 1: Encryption Policy Regime Space

trade-offs affecting information security and privacy differently, as well as the ability and reliability of law enforcement access to plaintext of encrypted data.

We organize the techniques in four categories: (a) circumvent protections; (b) regulate technology; (c) compel assistance; and (d) employ workarounds. These categories broadly reflect general approaches to enable law enforcement access and thus reduce encryption's impact on the law enforcement mission.

When choosing appropriate techniques or comprehensive encryption policy regimes, scalability of techniques is an important consideration. A technique needs to scale, otherwise it is, at best, an expensive solution for specialty cases. A second requirement is standardization of techniques. Some degree of standardization is necessary to allow for the effective use of the techniques as tools, for instance, to exchange and share data in a commonly understood format and/or through standard interfaces between the provider of the data and the requesting law enforcement agency. A third item, scope of techniques, is equally important. For example, why would mobile banking applications have key escrow when financial data can be obtained from the bank? Why would Supervisory Control and Data Acquisition (SCADA) systems controlling the power grid need key escrow? The computer security risks can be reduced if plaintext recovery is limited to the most necessary data and does not put at risk systems where there is limited investigative interest or an alternative way to obtain plaintext.

4.1.1.1 Circumvent Protections

Lawful Hacking: Also referred to as government hacking or equipment interference, a government agency gains lawful access to target data to obtain the plaintext of relevant information. Lawful hacking may exploit vulnerabilities or misconfigurations 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. Through lawful hacking, the government may retrieve an encryption key, acquire passwords via a key logger or install a mechanism for covert system access in the future. In addition, lawful hacking tools provide powerful online monitor capabilities to collect evidence and intelligence. Such tools can be employed on specific targets (e.g., a service or device used by a particular user), as well as groups of users of a particular service. As some lawful hacking may employ the exploitation of software vulnerabilities, the government's stance on vulnerability disclosure warrants attention.

Surreptitious updates describe a type of lawful hacking that exploits the update mechanisms of the operating system or of

Table 1: Overview of Techniques

Circumvent Protections	Lawful Hacking (including surreptitious updates)	Brute Force			
Regulate Technology	Design Mandates	Weaken Standards	Regulate Sale/Use	Export Control	
Compel Assistance	Compel Provider Assistance	Compel User Decryption			
Employ Workarounds	Analyze Metadata	Exploit Sensor Data	Adapt Conventional Police Methods	Data Localization	Liability

an application to gain covert access to a computer or other end device. Normally distributed to provide new functionality or to fix bugs and security vulnerabilities, update mechanisms could be co-opted by law enforcement.[51]

In order to preserve lawful hacking capabilities, a government may be tempted to withhold a vulnerability from disclosure, which may diminish overall cybersecurity. As lawful hacking relies on the successful exploitation of a software, configuration or human weakness, it may not deliver reliable law enforcement access. Uncovering and using a vulnerability may compromise the security of other systems in a disproportionate manner. On the other hand, hacking a single targeted device through a misconfiguration has no such impact. Finally, widespread hacking by numerous law enforcement agencies at many levels of government would be difficult to control and coordinate, particularly given the challenges of attributing the sources of cyber attacks.

Brute-Force Attacks: A brute-force attack consists of trying many possible keys or passwords until the correct key or password is found and the data is decrypted. The computing power required for a brute-force attack grows with increasing key length; adding one bit to the key doubles the strength of the algorithm to resist a brute-force attack. While today 64-bit keys can be brute-forced with a reasonable amount of computing power, 128-bit keys and beyond are generally considered unbreakable.[52] Thus, most successful brute force attacks involve weaknesses in the encryption algorithm or its implementation, particularly the robustness of key generation. For example, successful attacks on passwords often exploit the fact that users tend to employ non-randomized passwords. Attackers can consult dictionaries that contain millions of widely used passwords and combinations of characters, which allow experts, in some cases, to discover passwords within hours.[53]

4.1.1.2 Regulate Technology

Design Mandates: Government may require that providers and manufacturers design, build and deploy products and services with the capability to accommodate future lawful access requests. Various design techniques may be used to accomplish this objective. Design mandates have been used successfully for decades with most nations' telecommunications providers to ensure law enforcement's ability to conduct legal wiretaps.[54] For encryption, the government could mandate limits on cryptographic key lengths in commercial products and services. By limiting the maximum key length, a government could limit the effectiveness of encryption within a market or sub-market (e.g., sector-specific limitations). The permitted, but reduced, key length corresponds to the capabilities of a government to deploy brute-force attacks against encrypted data it wants to obtain. Of course, other well-resourced attackers could exploit this weakness.

[51] Note that the categorization of a technique depends on context. For example, "surreptitious updates" is a lawful hacking technique, if law enforcement employs it secretly by exploiting a broken key signing mechanism. However, if law enforcement compels a software vendor to execute a software update on a particular device (e.g., to install a covert access capability), this would put "surreptitious updates" in the category of compelled assistance.

[52] Orin Kerr and Bruce Schneier, Encryption Workarounds, Georgetown Law Journal, 2017 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033>.

[53] E.g., Dan Goodin, 'Anatomy of a Hack: How Crackers Ransack Passwords like "qeadzcwrsfxv1331"', Ars Technica, 27 May 2013 <https://arstechnica.com/information-technology/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/2/>.

[54] See section 4.1.2.3 for a description of CALEA.

A more fruitful approach might utilize key escrow, a method of recovering an encryption key. In a key escrow mechanism, a service provider and/or one or several third parties store decryption keys. If the government meets the legal requirements, it can request the escrowed key from the third parties to decrypt data or communications. The holder of the escrowed keys can be a service provider, one or more independent third parties or a government agency. To prevent the unauthorized use of the escrowed key by a third party (e.g., the escrow agent or an entity that stole the escrow key), the key can be split and stored in fragments. A split escrow key regains its functionality once a subset (e.g., 5 of 7) of the key fragments is rejoined.[55] Managing escrow keys can be complex and costly, especially if perfect-forward secrecy is used in which each communication or session generates a unique key. With the increasing number of breaches, including recent breaches of some of the most secure intelligence agency systems, particular attention is needed to limit the scope of any key escrow mandate in order to limit overall cybersecurity risk. Even with key escrow in place, users can potentially circumvent the key escrow mechanism by employing an additional level of encryption that has no shared decryption key.

Government design mandates would not need to specify the design mechanism used, only the decryption capability required, within the bounds of realism.

Weaken Cryptography Standards: Deliberately weakening cryptography standards through the voluntary international standards setting process can make an entire class of encryption susceptible to attack. Such weaknesses have been introduced covertly by governments in the process of designing and standardizing encryption standards. More localized impacts occur in cases where governments develop national standards. Such actions can disproportionately reduce cybersecurity when compared with law enforcement's needs. They also undermine confidence in standards setting processes and organizations.

Regulate the Sale and/or Use of Encryption: Governments may require a license for companies or users to sell or use certain encryption technologies. In order to receive a sale or use license, governments may require the encryption technology to be made available for technical inspection and review. This may allow a government to learn about the latest developments in the field and to stay ahead of the curve. To hinder adoption of an encryption technology in its jurisdiction, a government might simply deny a license and thus, effectively ban the encryption technology in question. In the context of apps that provide encryption to communications on smart devices, a government might request the removal of (or prohibit) apps from the distribution platform (e.g., Apple's App Store or Google Play).

Export Controls: National laws and international treaties (e.g., the Wassenaar Arrangement) aim to prevent the sales and transfer of encryption technology to certain foreign countries and adversaries. Control lists determine what technologies require a license to be exported (e.g., only those using shorter encryption key lengths in encryption to secure data confidentiality). Export controls provide a way to restrict some technology from being widely disseminated and later used against the exporting country. For a variety of reasons, export controls have proven ineffective in limiting criminal access to strong encryption products.

4.1.1.3 Compel Assistance

Compelled Provider Assistance: Law enforcement may legally require ICT service providers or manufacturers to help decrypt information stored in or passing through their products, services or devices. This may include technical assistance to decrypt, intercept, manipulate and preserve data, or, if permitted by law, to re-write firmware or software, or covertly install remote capabilities. For example, an Internet service provider (ISP) or cloud service provider offering encryption services (e.g., secure email storage) may have access to decryption keys in order to assist a customer who loses their keys. Similarly, a telecommunications service provider might be compelled to assist in manipulating traffic to facilitate the installation of a covert remote access tool to a computer controlled by a suspect under investigation. On the other hand, providers are increasingly offering products and services to which only the user has access to the decrypted information, limiting the effectiveness of compelling provider assistance. Moreover, some assistance may be quite expensive to implement, raising cost issues. Providers will also have concerns about potential legal liabilities for revealing customer data.

Compelled provider assistance differs from design mandates in that it does not require an ICT company to prospectively design and implement a decryption capability. Compelled provider assistance assumes that the provider will use its best efforts to assist law enforcement upon receiving a lawful access request. Policymakers should exercise care in designing compliance regimes (e.g., large fines for failure to deliver plaintext) so as not to create an indirect design mandate.

Compel User Decryption: The government may directly compel a user to grant law enforcement access to data. A user of a service or device might be compelled to disclose the passcode, to enter a biometric passcode (thumbprint, face) or to produce the decrypted data. A right against self-incrimination exists in many legal systems (e.g., the 5th Amendment in the U.S. Constitution) and may bar certain actions to compel a suspect to provide access to systems or decrypt data.[56]

4.1.1.4 Employ Workarounds

Workarounds describe ways of finding a substitute for plaintext in certain situations, or using non-technical methods to achieve access to the plaintext. These may include analyzing metadata, exploiting sensor data, adapting conventional police methods to the digital age, data localization and liability.

[55] This approach avoids creating single points of failure in the key escrow infrastructure.

[56] For a more detailed discussion of compelled assistance in the United States, see: Richard M. Thompson II and Chris Jaikaran, Encryption: Selected Legal Issues (Washington, D.C., 2016) <https://fas.org/sgp/crs/misc/R44407.pdf>.

Analyze Metadata: The analysis of metadata may provide important information about a subject and its communications, relationships and activities, and thus, support law enforcement investigations.[57] In communications, metadata is information about the sender and receiver of a call or email, duration of the communications, email addresses, dates, location and telemetry, but not the content of the communication. Other examples include the forensic analysis of metadata, such as the use of camera fingerprinting to compare encrypted data and unencrypted photographs both found on the same hard drive with data on the Internet (e.g., child exploitation videos) to subsequently link to a particular suspect.

Exploit Sensor Data: The expanding universe of home, commercial and industrial devices connected to the Internet contains a large number of sensors that collect audio, video and other data that can supplement traditional data gathering methods. A full public discussion has yet to take place about the legal, security and privacy implications of law enforcement collecting data from these sensors.

Adapt Conventional Police Methods: Governments may rely and even expand on traditional but tested practices to acquire passwords, decryption keys or plaintext by conducting surveillance, interrogating witnesses, recording confessions or conducting physical searches to obtain evidence. For example, conducting a physical search in a target office may retrieve a decryption key or login details. Alternatively, the plaintext might be retrievable from a communications intermediary or another party involved in the conversation. Depending on the specific circumstances, traditional methods may or may not be sufficient.

Data Localization: A government may require service providers to store certain data within a state's territory. Such a measure positions the data within the legal reach of the state, should a need for lawful access arise.

Liability: Providers of services and device manufacturers whose encryption services or products caused public harm (e.g., by making it impossible for law enforcement to prevent a crime), could be held civilly liable. In theory, such a liability could cause service providers and device manufacturers to modify the encryption in their services or products.[58]

4.1.2 Limitations on the Uses of Techniques

This section describes the second dimension of the framework. Divided into seven categories, Table 2 provides an overview of the conditions set by lawmakers and regulators that can limit the use of techniques to increase public trust in their use. They represent conditions that constrain the power of the state by limiting the effectiveness or efficiency of these techniques in order to mitigate the effects of using the techniques on privacy and other human rights, commerce, and innovation. These conditions assume effective institutional checks and balances are in place.

The conditions described here relate to some, but not all, techniques discussed in the previous section. For instance, requirements for transparency are broadly applicable to most techniques, whereas requirements for vulnerability disclosure relate specifically to the use of lawful hacking.

Effective limitations depend on appropriate oversight and enforcement. In practice, there have been cases where techniques have been misused by officials overstating their authorities or have been exploited by unauthorized third parties. Limitations alone are not a sufficient guarantor for lawful application of the techniques.

The limitations, implemented through legislative or regulatory means and enforced by executive and judicial authorities, help to ensure the accountable use of techniques within a legal framework in order to mitigate harmful effects on other values. In particular, the proper application and enforcement of limitations reduces the risk of:

- Non-authorized use of these techniques by law enforcement or third parties; and
- Unintended consequences or harmful collateral damage to systems whether or not they are related to the investigation.

[57] Although it relates to the now invalidated EU Data Retention Directive, a contemporaneous evaluation of the directive provides good insight in how metadata is used in criminal investigations and prosecutions. See, European Commission, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC) (Brussels, 2011) <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32006L0024>.

[58] U.S. Senator Sheldon Whitehouse brought up the question at a 2015 hearing whether ICT companies could be liable civilly when their services or products would harm public safety. See, Zoe Bedell and Benjamin Wittes, 'Civil Liability for End-to-End Encryption: Threat or Fantasy? Part I', Lawfare Blog, 2015 <https://www.lawfareblog.com/civil-liability-end-end-encryption-threat-or-fantasy-part-i>; and Jason Koebler, 'Senator: Crime Victims Should Be Able to Sue Apple, Google for Encrypting Data', Motherboard, 8 July 2015 <https://motherboard.vice.com/en_us/article/ezvw9z/senator-crime-victims-should-be-able-to-sue-apple-google-for-encrypting-data>.

Table 2: Overview of Limitations

Oversight	Transparency	Notification			
Due Process and Procedural Safeguards	Use of techniques subject to approval by an authority	Suppression of illegally obtained evidence			
Budgetary Constraints and Cost Reimbursement	Budgetary constraints on law enforcement	Cost reimbursement for up-front system modifications	Cost reimbursement of providing assistance		
Limitation to Types of Crimes, Devices or Services	Applicability to a limited list of serious crimes	Enumeration of covered devices and services			
Limitations of Use	Exhaustion	Particularity	Time limits	Minimization	Territorial limitations
Limitations to Third-Party Assistance	Determination of the scope of compelled assistance	Determination of what is a reasonable effort to comply with a request for technical assistance			
Vulnerability Disclosure	Vulnerability management	Disclosure policy and procedure			

4.1.2.1 Oversight

Transparency and notification requirements are key aspects in enabling oversight by the public and the government. The public, businesses and civil society can mobilize and engage in policymaking and lobbying efforts to strengthen governmental check and balance mechanisms.[59] The three branches of government exercise oversight as follows:

- The legislature, through formal oversight functions, committees and hearings;
- The executive, through independent inspector generals and regulatory oversight; and
- The judiciary, by requiring judicial review and other judicial means of due process.

Oversight can be public or private, the latter when oversight mechanisms are restricted to government-only, as with the U.S. Foreign Intelligence Surveillance Court.

Transparency about the use of techniques can be achieved through (public or private) summary reporting to the legislature by requiring courts and law enforcement to report the authori-

[59] For a discussion inter-branch checks and balances, see: Alan Rozenshtein, 'Surveillance Intermediaries', 2007 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2935321>.

zation and use of techniques. Similarly, corporations can be permitted or required to disclose government requests in the form of summary reporting or on a case-by-case basis. The annual wiretap reports to the U.S. Congress are an example of public (summary) reporting to the legislature of orders for interception of wire, oral or electronic communications.[60] Large ICT corporations, including Google, Microsoft and Twitter, release annual corporate transparency reports. Interestingly, the companies' transparency reports have revealed discrepancies regarding wiretap statistics released in the annual wiretap reports.[61] This makes the case for multiple, independent sources in the reporting to foster robust transparency. Further, transparency is gained when court proceedings concerning the use of techniques are in the open. If legal proceedings are initially sealed, a court should unseal the application after a set period unless law enforcement applies to continue sealing and shows sufficient cause.

Notifications sent to subjects to inform them that they were targeted in an investigation using legally approved techniques contribute to transparency and oversight. It helps to prevent the unaccountable use of techniques. Different types of required notices are conceivable, and the target may be informed before or after the techniques have been used. Time limits may determine when authorities must issue pre-notifications or post-notifications, and circumstances may warrant delayed notices. Under U.S. wiretap law, for instance, a notice is required within 90 days of the termination of the wiretap—as well as when the application for a wiretap order was rejected.[62] The notice provides whether the interception has been authorized or denied, the period of the interception and whether communications were intercepted.

4.1.2.2 Due Process and Procedural Safeguards

All democracies provide "due process," which refers to the protections for citizens from the arbitrary use of power by the state in legal proceedings. The use of techniques should be subject to approval by an entity independent of the investigating entity. Across democracies, such entities including judicial entities, maintain various degrees of independence from the investigative entities. In addition, there are variations in the kind of techniques they are legally competent to authorize, resulting in different thresholds for the investigating entity for a subpoena, warrant or other form of order. In the U.S., techniques that require a court order issued by a judge are subject to judicial oversight (an independent authority), whereas an administrative order signed off by an executive branch entity has a lower threshold and is a less effective limitation.[63,64] In cases where legal procedures and limitations are violated, the court may suppress evidence.[65]

4.1.2.3 Budgetary Constraints and Cost Reimbursement

The cost of provider compliance with a legal obligation to provide assistance or access to law enforcement can be reimbursed by the requesting entity. These costs may include: (1) the cost of developing, installing and deploying the required infrastructure to employ access techniques; and (2) a per request cost. In the U.S., for example, under the Communications Assistance for Law Enforcement Act (CALEA), telecommunication carriers can apply for cost-shifting relief (e.g., costs resulting from the carrier's CALEA compliance).[66] CALEA requires telecommunication carriers to deploy equipment that incorporates lawful interception capabilities.[67] For individual requests, communications providers have

[60] An annual Wiretap Report from the Administrative Office of U.S. Courts to the U.S. Congress is required under 18 U.S.C. § 3103a. For the reports, see, United States Courts, Wiretap Reports, 2016 <http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports>.

[61] For an analysis of this issue, see, Albert Gidari, 'Wiretap Reports Not So Transparent', The Center for Internet and Society, 2017 <http://cyberlaw.stanford.edu/blog/2017/01/wiretap-reports-not-so-transparent>.

[62] See, 18 U.S.C. § 2518(8)(d), 18 U.S. Code § 2518 - Procedure for Interception of Wire, Oral, or Electronic Communications <https://www.law.cornell.edu/uscode/text/18/2518>.

[63] For instance, under U.S. law, a wiretap requires a court order which is only issued if the judge determines that there is "probable cause"—among other requirements—that a crime is being committed, has been committed or is going to be committed. See, 18 U.S.C. § 2518(3)(a), 18 U.S. Code § 2518 - Procedure for Interception of Wire, Oral, or Electronic Communications.

[64] For a thorough treatment of U.S. law on government hacking see, Jonathan Mayer, Government Hacking, Yale Law Journal, 2018 <https://www.yalelawjournal.org/pdf/Mayer_k3iy4nv8.pdf>.

[65] See, 18 U.S.C. § 2515, 18 U.S. Code § 2515 - Prohibition of Use as Evidence of Intercepted Wire or Oral Communications <https://www.law.cornell.edu/uscode/text/18/2515>.

[66] See, 47 U.S. C. § 1008, CALEA § 109, 47 U.S. Code § 1008 - Payment of Costs of Telecommunications Carriers to Comply with Capability Requirements <https://www.law.cornell.edu/uscode/text/47/1008>. See, CALEA § 109(b)(1) Petitions for Cost-Shifting Relief. <https://web.archive.org/web/20160217204552/https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance>; Patricia Moloney Figliola, Digital Surveillance: The Communications Assistance for Law Enforcement Act (Washington, D.C., 2007) <https://fas.org/sgp/crs/intel/RL30677.pdf>.

[67] A 2006 U.S. Department of Justice Inspector General report on "CALEA Implementation Costs and Progress" noted: "After 10 years and the expenditure of over $450 million, the FBI estimates that only 10 to 20 percent of the wireline switches, and approximately 50 percent of the pre-1995 and 90 percent of the post-1995 wireless switches, respectively, have CALEA software activated and thus are considered CALEA-compliant. The FBI's strategy for spending these funds focused on identifying switches in locations of high-priority to law enforcement and first ensuring the CALEA-compliance of those switches. While the number of CALEA-compliant switches is based on the best available data, we cannot provide assurance on the accuracy of these estimates. Neither the FBI nor the FCC know the actual percentages of CALEA-compliance because the universe of carriers is unknown. In addition, as reported in previous OIG audits, the cost information provided to us by the FBI did not provide a basis to determine the reasonableness of the costs the FBI incurred." See, U.S. Department of Justice, The Implementation of the Communications Assistance for Law Enforcement Act, 2006 <https://oig.justice.gov/reports/FBI/a0613/findings.htm>.

charged law enforcement hundreds of dollars per target per month (e.g., T-Mobile charged a flat fee of $500 per target).[68] In 2012, U.S. cellphone providers received more than $20 million from law enforcement agencies for lawfully providing user information.[69] The use of technologies could be limited by capping the associated cost for reimbursement in the law enforcement agencies' budgets. Law enforcement authorities would have to make economic choices and prioritize when and how often they employ certain techniques.

Whether budgetary constraints and economic incentives work effectively as limitations largely depends on who bears the cost. Is it the company and their consumers or are the expenses covered and recouped from Congress in a line item in the law enforcement's budget? What costs qualify for cost-shifting (e.g., installation, maintenance of infrastructure, case-specific requests)? Some costs, such as reputational harm from complying with law enforcement requests, cannot be compensated monetarily (e.g., Apple argued in Apple vs. FBI that being forced to make the changes to the iPhone requested by the FBI would inflict reputational harm). Finally, some contend that the fees telecom operators collect under CALEA from lawfully providing requested data has created incentives to treat this as a service within their business model, given the significant amounts received. The effectiveness of economic constraints in limiting the use of techniques is highly dependent on what is reimbursed and how much money is available for such reimbursements.

4.1.2.4 Limitation to Types of Crimes, Devices or Services

The use of certain techniques can be limited to certain types of crimes, for instance the most serious crimes, and a technique may not be authorized for any other type of investigation. Types of crimes may be specified by law; for example, the U.S. wiretap law enumerates serious crimes that permit their use.[70] Similarly, the systemic effects on cybersecurity, commerce and human rights can be mitigated by strict limitations on the types of devices or services subject to access requirements or lawful hacking.

4.1.2.5 Limitations on Use

For some techniques, restrictions can be imposed to limit their use. This includes:

- **Exhaustion:** other, less intrusive techniques have been tried and failed before a more intrusive technique will be authorized;[71]
- **Particularity:** the particular use of a technique in an investigation cannot be overly broad but must be clearly defined and narrowly targeted to a type of communications and crime;[72]
- **Time Limits:** the use of a technique must be limited in time (e.g., 30 days), a technique cannot be endlessly used without independent oversight and appropriate reauthorization;[73]
- **Minimization:** the use of techniques and the gathering of extraneous data should be limited to the minimum amount necessary to achieve the narrow goals of the legal order;[74] and
- **Territorial Limitations:** the use of techniques may be restricted to territorial boundaries as extraterritorial applications may violate national and international law.

4.1.2.6 Limitations on Third-Party Assistance

Limitations on the scope and substance of compelled assistance can mitigate systemic negative effects on cybersecurity and other interests by limiting the assistance to particular cases and devices.

4.1.2.7 Mandatory Vulnerability Disclosure

Vulnerability management and disclosure policies provide ways to manage risk associated with the use, acquisition and disclosure of exploitable vulnerabilities for law enforcement purposes. While these vulnerabilities enable lawful hacking, they can also put all users at risk if the vulnerability becomes known and exploited by a third party. Vulnerability management and disclosure policies act as safeguards.[75] They may prescribe

[68] Andy Greenberg, 'These Are The Prices AT&T, Verizon and Sprint Charge For Cellphone Wiretaps', Forbes, 3 April 2012 <https://www.forbes.com/sites/andygreenberg/2012/04/03/these-are-the-prices-att-verizon-and-sprint-charge-for-cellphone-wiretaps>.

[69] Steven Nelson, 'Cell Providers Collect Millions From Police for Handing Over User Information', U.S. News and World Report, 9 December 2013 <https://www.usnews.com/news/articles/2013/12/09/cell-providers-collect-millions-from-police-for-handing-over-user-information>.

[70] See, 18 U.S.C. § 2516(1), 18 U.S. Code § 2516 - Authorization for Interception of Wire, Oral, or Electronic Communications <https://www.law.cornell.edu/uscode/text/18/2516>. It is worth noting that many of these limitations cannot be applied for all proposed techniques. One could not limit the effects of weakening encryptions standards to only serious crimes. By contrast, one could limit lawful hacking to serious offenses, much like wiretapping is handled.

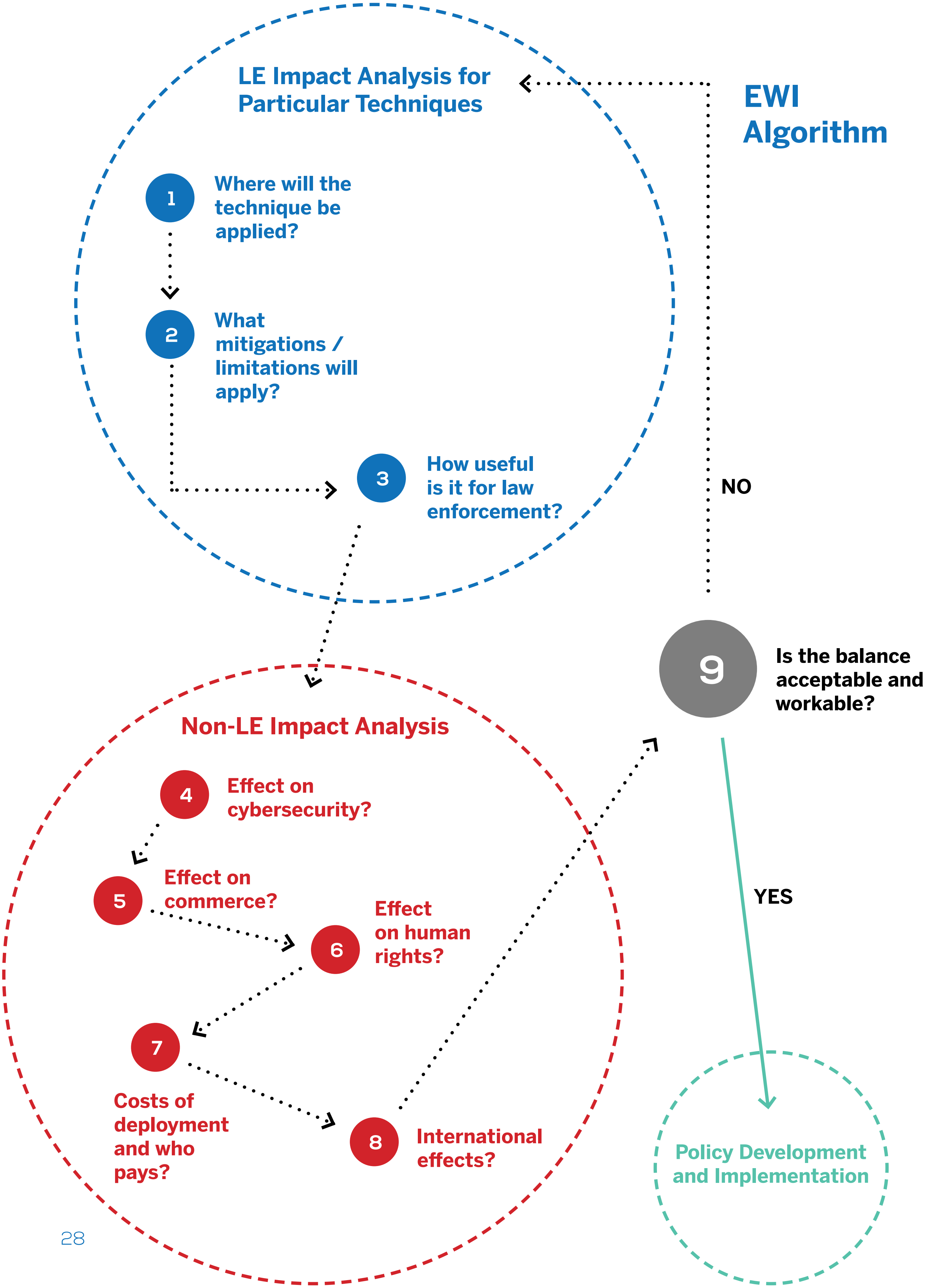
[71] For a legal example, the U.S. wiretap act states, "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(3)(c).

[72] For a legal example, the U.S. wiretap act states, "a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates." 18 U.S.C. § 2518(4)(c).

[73] For a legal example, the U.S. wiretap act states, that the intercept cannot be "longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days." 18 U.S.C. § 2518(5).

[74] For a legal example, the U.S. wiretap act states that the intercept "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception." 18 U.S.C. § 2518(5).

[75] Privacy International, 'Government Hacking and Surveillance: 10 Necessary Safeguards,' 2017 <https://privacyinternational.org/node/957>.



EWI Algorithm

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?

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?

9 Is the balance acceptable and workable?

NO

YES

Policy Development and Implementation

strict procedures and criteria to determine when a vulnerability must be withheld for law enforcement use or disclosed to fix the security weakness. A policy may also describe how and when a vulnerability must be reported after law enforcement learns about its existence. Further mitigation can be achieved by prescribing constraints to the procurement and operational deployment of vulnerabilities (e.g., what types of exploitable vulnerabilities or tools can be acquired by law enforcement, from whom can these be bought, and under what conditions are 0-day or n-day vulnerabilities deployed). However, limitations constrain law enforcement's ability to use vulnerabilities for lawful hacking. The U.S. federal government has a vulnerabilities equities process (VEP) to examine whether software vulnerabilities should be disclosed or withheld.[76] Federal agencies representing law enforcement, national security, diplomatic, economic and cybersecurity interests debate and agree on the final assessment (or the White House resolves disagreements). Restrictions may also come in the form of safeguards to prevent theft or leaks of powerful lawful hacking tools and vulnerabilities as they may lead to dire consequences. Some undisclosed vulnerabilities may be discovered independently and revealed, or stolen and leaked, with subsequent exploitation. To give an example, the 2017 WannaCry and NotPetya malware attacks made use of techniques that many believe were stolen from the U.S. National Security Agency (NSA), using code that exploits software vulnerabilities previously unknown to the public.[77]

4.1.3 ICT Environment

The ICT environment describes the overall infrastructure, equipment and devices that process, store and transmit data. It describes, in a schematic sense, where data resides. From there, one can determine how to access unencrypted and encrypted data (e.g., intercept for communications or data extraction for stored data on an end device). Data can be stored in an end device, such as a laptop, smart phone or external hard drive, or on the network on a server or in the cloud. Communications pass through the infrastructures and networks of Internet service providers and telecommunications providers. Data may exist simultaneously in multiple locations, for instance, when a backup copy of data on a user's device is stored in the cloud. Multiple copies may also exist for operational and technical purposes controlled by a service provider or vendor of an app. Data in transit is often packetized and takes different routes, only to be reassembled at the receiving end. Stored data can also be "sharded"—broken up into pieces and stored in multiple locations.

In the context of lawful access and encryption, often two general categories of data are distinguished:[78]

- Data at rest: data that is stored on a computer, smart phone, end device, server, in the cloud, or on other networked devices, in various files and formats; and
- Data in transit ("communications"): data that is moving across public or private networks and the Internet. Data in transit also includes voice, VoIP and data communications.

These different categories of data are not always clearly distinguishable; data that was just transmitted through an intermediary can become permanently stored on an end device and as such "change" its category. [79]

Data comes in different formats, including actual content (in the form of text, audio, video, images, and sensor data); metadata that describes data or properties of an information object, geolocation, application files, configuration files or systems logs; and passwords and encryption/decryption keys. The data itself can belong to a user or a third party, exist on a device owned and controlled by the user or a third party.

Law enforcement may request access to data from the sender, receiver, communications intermediary who transmitted the data, or service provider, device manufacturer or software vendor/application provider. Some of these entities may be located in foreign jurisdictions (e.g., the decryption key might be held by a person or organization abroad, the provider of an encrypted messaging app might be incorporated abroad with no domestic offices), complicating the process for lawful access. The involvement of multiple jurisdictions goes beyond the matter where the data is stored.[80]

Indeed, the ICT environment is not limited to technology; rather, it reveals key questions with respect to legal jurisdiction: (1) where is the data; (2) who has the key(s); (3) where are the person(s) with access to the data; (4) where is the service and/

[76] The White House, Vulnerabilities Equities Policy and Process for the United States Government (Washington, D.C., 2017) <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>.

[77] Alex Hern, 'WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017', The Guardian, 30 December 2017 <https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware>.

[78] Note: another type of data is "data in use," or data that is being processed. In most cases, in order to process data, it cannot be encrypted. In some cases, law enforcement aims at intercepting or capturing "data in use" at a particular point of time to ensure its accessibility, as otherwise, it is encrypted and not accessible for law enforcement. See, Dave Shackleford, 'Regulations and Standards: Where Encryption Applies', SANS Institute, 2007 <https://www.sans.org/reading-room/whitepapers/analyst/regulations-standards-encryption-applies-34675>.

[79] As one expert mused, "Is an email or file that is waiting on a mail server to be downloaded data at rest or data in transit? One could argue both ways. One might say only the SSL connection is actually the transit protection layer and hence it is in transit from sender to server and from server to receiver, but at rest on the server. Or one could see PGP encryption as transit protection, arguing that the entire time from sender to receiver can be considered as one end-to-end transit process."

[80] Elements of the crime or terrorist act might have been committed in multiple jurisdictions.

or telecom provider situated; (5) where is the victim; (6) from what jurisdiction is the investigation being conducted; and (7) what jurisdiction's laws should govern access to the data?

Data can be stored in multiple jurisdictions and communications may travel unexpected routes—often without the knowledge of and outside the control of the user. For instance, data stored in the cloud might be transferred to other instances of the cloud for operational purposes, changing the physical location of where the data is stored, and with it, changing the legal protections based on the jurisdiction of the physical server location. In communications, so-called boomerang routing[81] might route a call or electronic communications abroad, even if the call or the communications is originating (sending) and terminating (being received) in the same domestic city. The communications might be routed abroad and with it, lose all protections guaranteed under the domestic legal framework and become potentially available for intercept in a jurisdiction with lower levels of protections.[82]

4.2 The EWI Algorithm

To assess policy options—individual ones and their aggregate as encryption policy regimes—EWI devised a systematic, structured methodology to focus discussion. The methodology (algorithm) helps to identify both similarities and differences across different groups steering towards balanced solutions.

The algorithm enables consideration of interests across six domains:

1-3. Law Enforcement: Usefulness and effectiveness for law enforcement
4. Cybersecurity: Intended and unintended effects on cybersecurity
5. Commerce: Intended and unintended economic effects for the ICT industry (innovation, international trade) and businesses (efforts and cost of compliance, costs of non-compliance)
6. Human Rights: Intended and unintended effects on privacy and other human rights
7. Deployment Cost and Cost Coverage: Costs of deployment and cost allocation
8. International Ramifications: Intended and unintended international effects

The key steps in the algorithm are described in Figure 2.

4.2.1 Key Steps in the EWI Algorithm

Implementation of the EWI algorithm consists of two parts—law enforcement (LE) impact analysis and non-LE impact analysis—and an assessment of whether a policy option or an encryption policy regime is balanced. Generally speaking, the process can be used in two ways: (1) an open, unstructured approach, where the expert group builds an encryption policy regime from the ground up, exploring all possible options; or (2) a structured, scenario-based approach where the facilitators provide an initial encryption policy regime which the experts use to work through. For this report and the formulation of the sample regimes, EWI opted for the latter approach.

Below is a description of the key elements of the EWI Algorithm:

LE Impact Analysis for Particular Techniques: Steps 1-3

- Step 1: Determine where in the ICT environment there is a need for access to encrypted data; select a technique.
- Step 2: With regard to the technique, determine what limitations will be applied.
- Step 3: Determine how useful, effective and efficient the proposed technique is in combination with the limitation to gain access to encrypted data in plaintext.

Non-LE Impact Analysis: Steps 4-8

The non-LE analysis is based on structured, consecutive discussions of each of the five non-LE elements. The algorithm does not prescribe a particular assessment model or framework for each element but rather relies on the expertise of the participants.

Assessment: Threshold Test: Step 9

The group decides whether a particular policy option or encryption regime is deemed "acceptable" and "workable." The algorithm does not provide a method to measure or determine the group consensus. If after several iterations no rough consensus can be established, the EWI process proposes to write up a statement that incorporates the majority view and several dissenting statements. The process then moves forward. Unsettled policy options can be revisited at a later point.

Policy Development and Implementation

The EWI algorithm does not eliminate the challenges attendant to developing and implementing detailed statutory or regulatory encryption policies. It provides a substantive basis for those processes. The algorithm's results may change over time due to technological innovation and national and international legal and political developments.

[81] Internet Boomerang Routing: "Boomerang routing refers to internet routing where a data path starts and ends in the same country (e.g. Canada) but passes through another country (e.g., the U.S.) before returning. This is a common occurrence with Canadian internet communication." IX Maps, 'Glossary' <https://www.ixmaps.ca/learn/glossary.php>.

[82] Andrew Clement and Jonathan Obar, 'Keeping Internet Users in the Know or in the Dark: An Analysis of the Data Privacy Transparency of Canadian Internet Carriers', Journal of Information Policy, 6 (2016), 294–331 <http://www.jstor.org/stable/10.5325/jinfopoli.6.2016.0294>.

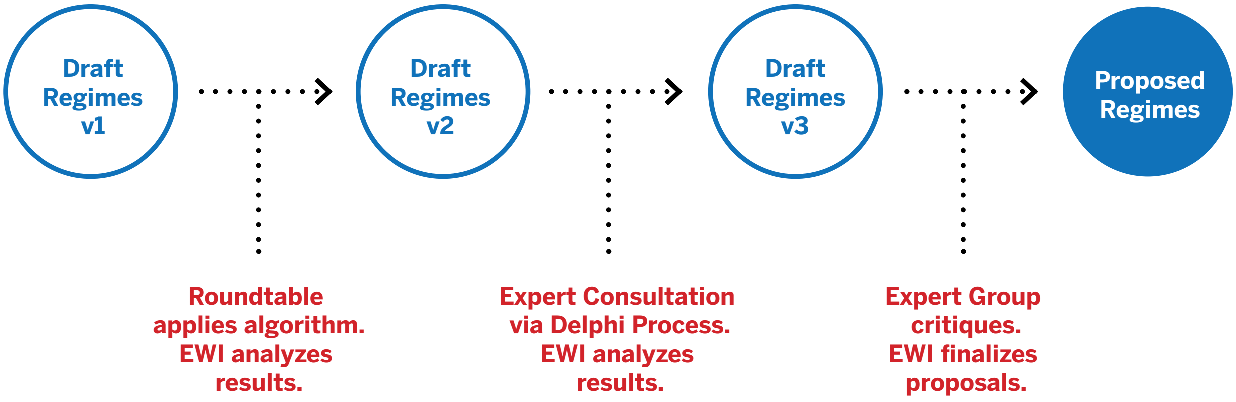

Draft Regimes v1
Draft Regimes v2
Draft Regimes v3
Proposed Regimes
Roundtable applies algorithm. EWI analyzes results.
Expert Consultation via Delphi Process. EWI analyzes results.
Expert Group critiques. EWI finalizes proposals.

Figure 3: Regime Refinement Process from Draft to Proposed Regimes

4.3 A Structured Process: the Delphi Method

There is a lack of empirical data on the potential impact and effectiveness of encryption policies on law enforcement's access to data, and of the public safety impacts of varying degrees of access. More empirical data is needed. In the meantime, EWI recommends using a variation of the Delphi method to obtain normative and practical feedback on encryption policy regimes.

The Delphi method was originally developed by the RAND Corporation to poll and aggregate the opinions of experts in a particular field in order to reach a consensus and "predict the future." It is most useful in cases, such as this, where there are many unknown factors and when the problem requires significant levels of expertise. The process involves surveying a group of experts, ideally around 10 to 18, from diverse backgrounds (e.g., government, civil society, academia and industry). Below is a summary of the steps involved in a typical Delphi process:

1. Formulation of the issues: what is the issue that really should be under consideration? How should it be stated?
2. Exposing the options: given the issue, what are the policy options available?
3. Determining initial positions on the issues: which are the ones everyone already agrees upon and which are the unimportant ones to be discarded? Which are the ones exhibiting disagreement among the participating experts?
4. Exploring and obtaining the reasons for disagreements: what underlying assumptions, views or facts are being used by the individuals to support their respective positions?
5. Evaluating the underlying reasons: how does the group view the separate arguments used to defend various positions and how do they compare to one another on a relative basis?
6. Reevaluating the options: reevaluation is based upon the views of the underlying "evidence" and the assessment of its relevance to each position taken.

The process is designed to expose the differing positions and the principal pro and con arguments for those positions.[83]

4.4 How EWI Used the Framework to Develop Proposed Policies

EWI applied the framework to develop the two proposed encryption policy regimes described in Section 5. EWI conducted three rounds of consultation. In each round, EWI used the algorithm to evaluate the proposed encryption regimes. EWI submitted draft encryption regimes to experts, who evaluated the regimes' effects according to the algorithm.

The first round utilized an in-person workshop among some 30 members of EWI's global cyber policy network. The second round used a survey with extensive briefing materials and telephone conversations to engage 10 encryption policy experts representing law enforcement, private industry, academia and civil society from the United States, Europe and India.[84] A third round with some of the same and some new experts concluded the process. Based on this feedback, EWI adjusted the draft regimes, but did not attempt to find consensus on the "right" mix of techniques and limitations. Indeed, there was strong disagreement on the policy merits of some proposed approaches. The regime refinement process is illustrated in Figure 3. A summary of the substantive discussion and comments that led to the formulation of the proposed regimes is provided in the appendix.

[83] Murray Turoff, 'The Policy Delphi', in The Delphi Method: Techniques and Applications, ed. by Harold A. Linstone and Murray Turoff, 2002, pp. 80–96.

[84] A balanced composition of experts in the Delphi process is crucial. A one-sided selection is likely to lead to biased recommendations that fail at the outset to have any claim to broad legitimacy.

5 Balanced Encryption Policy Regimes

The two regimes highlight a key choice that policymakers face—enhancing law enforcement's ability to covertly access systems relevant to investigations, or requiring action by ICT companies to design their systems to anticipate requests for lawful access. Each approach would represent a change in current law in policy in most democracies, and each has upsides and downsides for all the various interests at stake. The regimes need not be mutually exclusive. A nation could pick and choose elements from each, or decide that no change in current law or policy is merited. The proposed regimes provide a baseline for improved national and international discussion and cooperation.

Each regime consists of a set of techniques,[85] each conditioned by certain limitations,[86] applied across three relevant technology environments.[87,88] In addition, systemic improvements are recommended to improve law enforcement's overall effectiveness in dealing with digital evidence. The following table provides an overview of the two proposed Encryption Policy Regimes; the remainder of this section describes each regime in detail.

5.1 Proposed Regime 1: Lawful Hacking (with Compelled Provider Assistance)

5.1.1 Compelled Provider Assistance (for data stored in the cloud, on an end device and communications)

For data at rest (i.e., in the cloud or on an end device), consistent with applicable national law, law enforcement entities may compel assistance[89] from any private party ("data custodian") who may have legal access to stored encrypted data in order to facilitate access to the plaintext of the stored data, and to metadata and logs related to the stored data, under the following limitations:

- Costs of assistance shall be reimbursed by the requesting entity;
- The order to provide assistance is approved by an independent judicial authority;
- The requesting entity or the data custodian shall notify the subject of the investigation or other data owner prior to accessing the data, unless the independent judicial authority specifically authorizes delaying or withholding notification; and
- In case of data stored on an end device (e.g., smart phone), the device shall be in the physical possession of the requesting entity.

For data in transit, law enforcement entities may compel assistance from communication services providers (e.g., telecom operators, ISPs, over-the-top communication services provid-

[85] Techniques are methods that enable law enforcement to obtain lawful access to the plaintext of encrypted information by: (1) circumventing security protections; (2) regulating encryption technology; (3) compelling assistance from providers or from targeted users; and (4) working around the encryption by other means.

[86] Limitations are ways of limiting the impact of the techniques on non-law enforcement-specific interests, including robust cybersecurity, a vibrant ICT market, businesses and innovation, protection of human rights, economic efficiency, and cooperative international relations.

[87] The three technology environments comprise data stored in the cloud, data stored on an end device, and communications (data in transit). For the purpose of the proposed regimes, we differentiate between "data at rest" and "data in transit," recognizing that boundaries between technology environments are increasingly blurry. We also note that multiple entities may possess copies of the requested data.

[88] To deal with cross-border jurisdictional issues, the analysis points to MLATs and other bilateral agreements for lawful access in foreign jurisdictions. Cross-border jurisdictional issues are complex as they implicate questions regarding the legal and physical location of: the data, the key, the subject of the investigation, the provider, the victim, the crime scene, and the requesting law enforcement entity. These aspects are common components of more complicated use-cases, along with the time sensitivity of a case (imminent threat), and the severity of the respective crime.

[89] See definition of compelled provider assistance in section 4.1.1.3.

	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						

Table 3: Overview of Proposed Regimes

ers), in accordance with their role in the data transmission process[90] and subject to rules of international legal jurisdiction. Such assistance may include data interception and other technical and other assistance that will facilitate access to the plaintext of encrypted data, and to metadata and logs related to the transmission.

For both data at rest and communications, compelled provider assistance applies to data and communications encrypted using techniques provided by the device manufacturer or services provider. There is no obligation to assist with decryption of data obfuscated by a third party, such as an over-the-top encrypted or ephemeral messaging service. If such third-party encryption is involved, assistance must be compelled from the respective provider directly.

In cases where any device manufacturer or services provider has no access to means of decryption (e.g., having rendered the decryption key exclusively to the user), they may be required to provide technical assistance to circumvent the protections in alternative ways, subject to necessity and proportionality. Compelled provider assistance is not a design mandate in which system architecture is required to be altered in anticipation of future lawful requests for technical assistance.

5.1.2 Lawful Hacking (for data stored in the cloud, on an end device and communications)

If the compelled provider assistance does not produce the plaintext of the encrypted data, the requesting entity may utilize lawful hacking[91] to retrieve relevant data at rest or communications (including cameras or other sensors, to the extent legally permitted). Lawful hacking may be used by a law enforcement entity to gain access to the plaintext of data or communications under the following limitations:

- The use of the techniques is approved by an independent judicial authority;
- Vulnerabilities in software or hardware used for lawful hacking are subject to a transparent vulnerabilities equities process, which determines whether such vulnerabilities must be disclosed to the software vendor and/or the public, or can be kept concealed for lawful hacking purposes for a limited amount of time. No limitations apply to the use of publicly reported vulnerabilities;
- The entity shall notify the subject of the investigation promptly upon achieving access to the plaintext, unless the independent judicial authority specifically authorizes delaying or withholding notification; and
- Law enforcement shall provide periodic, public summary reports about its use of lawful hacking techniques to an independent governmental oversight body.[92]

5.2 Proposed Regime 2: Design Mandates (with Compelled Provider Assistance)

Regime 2 eliminates Lawful Hacking in favor of limited Design Mandates.

5.2.1 Compelled Provider Assistance (for data stored in the cloud, on an end device and communications)[93]

For data at rest (i.e., in the cloud or on an end device), consistent with applicable national law, law enforcement entities may compel assistance[94] from any private party ("data custodian") who may have legal access to stored encrypted data in order to facilitate access to the plaintext of the stored data, and to metadata and logs related to the stored data, under the following limitations:

- Costs of assistance shall be reimbursed by the requesting entity;
- The order to provide assistance is approved by an independent judicial authority;
- The requesting entity or the data custodian shall notify the subject of the investigation or other data owner prior to accessing the data, unless the independent judicial authority specifically authorizes delaying or withholding notification; and
- In case of data stored on an end device (e.g., smart phone), the device shall be in the physical possession of the requesting entity.

For data in transit, law enforcement entities may compel assistance from communication services providers (e.g., telecom operators, ISPs and over-the-top communication services providers), in accordance with their role in the data transmission process[95] and subject to rules of international legal jurisdiction. Such assistance may include data

[90] For example, telecom operators or ISPs may be able to provide access to the data traffic and, where technically feasible, separate traffic associated with specific applications out of the general traffic (e.g., by using deep packet inspection and similar techniques). Over-the-top (OTT) providers may be able (subject to technical feasibility) to assist in decrypting the captured traffic.

[91] See section 4.1.1.1 for definition.

[92] Additional conditions worth considering include: law enforcement must make sure that after the operation is finalized the integrity of the targeted device is restored.

[93] This subsection is identical to Compelled Provider Assistance in Regime 1, Section 5.1.1.

[94] See definition of compelled provider assistance in section 4.1.1.3.

[95] For example, telecom operators or ISPs may be able to provide access to the data traffic and, where technically feasible, separate traffic associated with specific applications out of the general traffic (e.g., by using deep packet inspection and similar techniques). Over-the-top (OTT) providers may be able (subject to technical feasibility) to assist in decrypting the captured traffic.

interception and other technical and other assistance that will facilitate access to the plaintext of encrypted data, and to metadata and logs related to the transmission.

For both data at rest and communications, compelled provider assistance applies to data and communications encrypted using techniques provided by the device manufacturer or services provider. There is no obligation to assist with decryption of data obfuscated by a third party, such as an over-the-top encrypted or ephemeral messaging service. If such third-party encryption is involved, assistance must be compelled from the respective provider directly.

In cases where any device manufacturer or services provider has no access to means of decryption (e.g., having rendered the decryption key exclusively to the user), they may be required to provide technical assistance to circumvent the protections in alternative ways, subject to necessity and proportionality. Compelled provider assistance is not a design mandate in which system architecture is required to be altered in anticipation of future lawful requests for technical assistance.

5.2.2 Design Mandates (for smart devices, cloud data, and designated ephemeral messaging and encrypted messaging services)

In Regime 2, design mandates[96] would require that providers and manufacturers design, build and deploy products and services with the capability to accommodate future lawful access requests to provide access to plaintext in the circumstances below and under the following general conditions:

- One-time costs of designing and creating the capability shall be reimbursed by the national government, and costs of assistance shall be reimbursed by the requesting entity;
- The law enforcement entity's request is subject to prior approval by an independent judicial authority;
- The requesting entity shall notify the data owner prior to accessing the data, unless the independent judicial authority specifically authorizes delaying or withholding notification; and
- Design mandates are imposed through a public (i.e., non-secret) regulatory process.

Smart device manufacturers are required to be able to produce, within 48 hours, the plaintext of data resident on a smart device[97] under the general conditions above and:

- The device is in the lawful physical possession of the requesting entity; and
- Data on the smart device that was encrypted using service provided by a third party is not subject to this requirement, nor does the mandate include a ban on the manufacture and use of third-party encryption.[98]

Cloud data service providers that encrypt customer data are required to have the capability to recover and provide, within 72 hours, the plaintext of data of named customers' accounts if served with judicial authorization valid in the provider's jurisdiction under the general conditions above.[99]

Designated ephemeral and/or encrypted messaging services providers are required to have the capability to back up the data of named users/accounts if served with judicial authorization valid in the provider's jurisdiction. Providers of designated services subject to this design mandate are required to produce the requested data to law enforcement authorities within 72 hours under the general conditions above, and:

- The list of designated services under this provision is subject to annual recertification by the executive branch; and
- An independent advisory committee assesses the security and human rights implications of the design mandate and advises the executive branch accordingly.

5.3 Systemic Improvements

Systemic improvements that benefit law enforcement authorities' overall efforts regarding combating cyber-enabled crime and terrorism are applicable to both proposed regimes.

[96] See discussion at 4.1.1.2.

[97] One schematic functioning of this mechanism: the user's private key to decrypt the data is securely stored on the device and is encrypted with the public key of the manufacturer and the public key of the national law enforcement agency. Under this key recovery mechanism, to gain access to a user's private key to decrypted data, both the private key of the law enforcement agency and the private key of the manufacturer are needed.

[98] One expert noted that this provision could require device manufacturers to inhibit the installation of third-party encryption applications on their device.

[99] Many cloud service providers already operate key recovery mechanisms as part of their service and business model to assist a customer who loses a key or password.

5.3.1 Conduct Capacity Building for Law Enforcement

National governments should invest in capacity building for national and local law enforcement entities, including judiciary entities, to improve their ability to handle encrypted and unencrypted data of all types relevant to their mission. This includes:

5.3.1.1 Enhanced Forensic Capabilities

Law enforcement authorities, consistent with applicable national law, should develop and maintain state-of-the art capabilities and capacities for data decryption and alternative investigative techniques. To develop and make these capabilities available to national and local law enforcement entities, the respective authorities should, for example: develop and maintain a network of technical experts; provide training programs regarding the handling of encrypted data and digital evidence; and periodically assess the technical development and use of encryption technology by criminals.

5.3.2 Streamline the MLAT Process

National governments should work to streamline the processes for mutual legal assistance where data is being requested in foreign jurisdictions. In particular:

5.3.2.1 Reciprocal Access in Foreign Jurisdiction under MLAT

For relevant data located outside the domestic jurisdiction, law enforcement authorities may use established MLAT processes to gain lawful access to plaintext that is available to a law enforcement entity in the foreign jurisdiction under the following conditions:

- Public annual reporting to the legislative branch of the numbers of incoming and outgoing MLAT requests related to access to plaintext; and
- Periodic review of human rights implications of encryption-related requests.

Many national authorities are working towards streamlining the MLAT process, as it can be too slow and cumbersome to meet law enforcement needs in the digital era.

5.3.2.2 Bilateral Agreements Providing Due Process Equivalency

For relevant data located outside of the domestic jurisdiction, states may establish bilateral agreements to enable efficient lawful access to data and communications in a foreign jurisdiction. Such bilateral agreements would streamline the existing MLAT process between participating countries.

Bilateral agreements[100] may be used by a law enforcement entity to gain access to communications or stored data in or subject to foreign jurisdictions under the following limitations:

- Domestic legal requirements provide a reasonable protective standard for (foreign) lawful requests in the domestic jurisdiction;
- Public annual reporting to the legislative branch of the numbers of requests (to and from foreign law enforcement authorities) under the bilateral agreement; and
- Annual recertification of the bilateral agreement by the executive branch.

5.3.3 Enhance Law Enforcement/Private Sector Cooperation and International Law Enforcement Cooperation

National governments and the private sector should work together to create an environment that fosters better cooperation between law enforcement (as well as, where relevant, data protection agencies and the judiciary) and private sector entities, particularly pertaining to the management of law enforcement requests and sharing of relevant data for preventive and investigative law enforcement purposes—nationally and internationally.

[100] Bilateral agreements between states with similar legal regimes and standards enable incoming foreign lawful access requests to be treated as if the law followed in the requesting nation was equivalent to the law followed in the nation receiving the request. Under such an agreement, for instance, a foreign law enforcement authority can serve (via the domestic law enforcement authority) a lawful request to a domestic entity in possession of the communications or stored data and compel assistance to provide access to the data, and vice versa. In July 2016, the U.S. government drafted a legislative proposal for a potential U.S.-UK agreement. See, David Kris, 'U.S. Government Presents Draft Legislation for Cross-Border Data Requests', Lawfare Blog, 2016 <https://www.lawfareblog.com/us-government-presents-draft-legislation-cross-border-data-requests>; and Tiffany Lin and Mailyn Fidler, 'Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement', Berkman Klein Center, 2017 <https://cyber.harvard.edu/publications/2017/09/berklett>.

6 Recommendations

The two proposed regimes are provided as illustrations of balanced approaches that EWI believes are generally consistent with these recommendations and are the outcome of an expert consultation aiming to identify common ground, but not necessarily consensus.

The following recommendations summarize the normative conclusions developed in this report.[101] The two proposed regimes are provided as illustrations of balanced approaches that EWI believes are generally consistent with these recommendations and are the outcome of an expert consultation aiming to identify common ground, but not necessarily consensus.

In the following recommendations:

- "Must" indicates that a recommendation is required to establish a balanced regime; and
- "Should" indicates that a recommendation is highly useful but can be modified or ignored when the full implications of its absence are understood and/or alternative means are put in place to mitigate negative effects.

A short commentary complements each recommendation with a rationale. The recommendations are listed from general to specific and help to advise the formulation of balanced regimes. Recommendations 1 through 3 and 9 are generally applicable, whereas recommendations 4 through 8 are relevant to specific policies or issues. Note that the analytical framework developed earlier in this report provides a more extensive description of the techniques and limitations. As the purpose of the recommendations is to provide general guidelines, they are deliberately lacking specific prescriptions (e.g., detailed limitations) and as such, need to be developed for each institutional setting.

1) Strong Cybersecurity

Governments must support and enable strong encryption and other digital protections to promote strong cybersecurity. Governments must refrain from policies and measures that systematically and broadly undermine cybersecurity for all users, including weakening or undermining cryptographic standards, introducing surreptitious access mechanisms into commercial, mass-market ICT products and services, restricting key lengths of cryptographic algorithms, requiring providers to maintain a copy of data in the clear, banning the use of products or services employing encryption, or generally mandating key escrow mechanisms. Specific measures to enable targeted access to data of particular users or services may be permissible under clearly defined circumstances, balanced considerations (i.e., under the application of the principles of proportionality, necessity and legality) and scope of targeted systems (e.g., excluding certain types of systems, such as SCADA systems or banking systems in which governments have no investigative interest or an alternative way to obtain access to data).

EWI Commentary: Encryption has been recognized as essential to cybersecurity to ensure privacy and the protection of personal and business data, communications and national security.[102] Strong cybersecurity is equally

[101] This conclusion does not imply legal harmonization across democracies as underlying values and drivers for encryption policy-making may differ. Yet, technique use and technical aspects might be the same and would allow for technical standardization (see also the note on Technical and Operational Standardization in the recommendation on infrastructure improvements).

[102] See, U.S. House Judiciary Committee and the House Energy and Commerce Committee.

important for citizens, businesses and the government, including law enforcement. Therefore, governments must take active measures to protect private and privileged data and communications, where such protection is required, and support and enable the use of strong encryption technology as appropriate. Strong encryption is supported by various international and governmental entities. For instance, the European Union confirmed that "strong and trusted encryption is highly important for properly ensuring human rights and fundamental freedoms," while recognizing the impediments law enforcement authorities are facing as a result of strong encryption and anonymization technologies.[103] Also, international bodies, such as the United Nations[104] and states such as The Netherlands,[105] have issued statements in support of encryption and against restrictive measures that undermine the protection encryption confers. In the U.S., the Encryption Working Group of the House Judiciary Committee and the House Energy and Commerce Committee concluded that "any measure that weakens encryption works against the national interest."[106] Due to wide-ranging implications for cybersecurity, national security as well as privacy and other human rights, policies that systematically undermine encryption must be avoided. Measures that enable access to decrypted data must be targeted, narrowly defined and embedded in a legal framework with adequate legal limitations (e.g., necessity and proportionality of measures). The overall importance of encryption for cybersecurity and resulting consequences for other interests might eventuate in law enforcement's inability to obtain access to encrypted data in some cases. Yet, targeted measures should reduce these impediments to the degree possible, but without undercutting the benefits of encryption for cybersecurity at large. Moreover, governments should allow a broad measure of freedom to their citizens to apply digital protections at their discretion, including allowing citizens to communicate anonymously. Digital protection, such as anonymous communications and steganography, should be preserved for future applications.

2) Balanced, Transparent, Risk-Informed Regimes

Governments must create balanced, transparent,[107] risk-informed,[108] and technology-neutral regimes for encryption

[103] Council of the European Union, 'Council Conclusions of 20 November 2017 on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU', 2017 <http://www.consilium.europa.eu/media/31666/st14435en17.pdf>; and European Commission, '2017 Eleventh Progress Report towards an Effective and Genuine Security Union', 2017 <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf>.

[104] United Nations Office of the High Commissioner, 'Report on Encryption, Anonymity, and the Human Rights Framework', 2017 <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>.

[105] ENISA; Dutch Ministry of Security and Justice.

[106] U.S. House Judiciary Committee and the House Energy and Commerce Committee.

[107] Transparent both in terms of clear linkage between statutory authorities and programmatic activities, and periodic reporting on the use of those authorities.

[108] The risk of particular encryption regimes is mitigated by the selection of techniques and limitations under balanced consideration of the needs and interests of government, business and civil society within a democratic decision-making process.

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 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. Further, regimes must reflect the input of a full, diverse set of stakeholders and interests, including those traditionally underrepresented. Governments must be responsible in protecting the public by being transparent about the trade-offs that have been made under particular encryption policies, and must inform the public about the impact of such trade-offs and the ways they may lower security protections.

> EWI Commentary: Trade-offs in encryption regimes should be informed by risk considerations and aim at an overall fair, balanced outcome for governments, businesses, the economy and civil society. Determining this balance and the appropriate levels of risk (i.e., which risks are deemed acceptable or not in a regime) is essential in making trade-offs in an encryption policy regime. This report acknowledges the difficulties in calculating certain types of risk that inform balanced trade-offs among stakeholders with competing interests and needs through a democratic process. As a result of the process, a regime might be biased toward particular interests and needs (e.g., cybersecurity, public safety or others) but also be subject to changes over time due the periodic reevaluations. Trade-offs may result in beneficial outcomes for one domain at the expense of one or several other groups, who might confront undesired or even negative effects. The balancing needs to occur across the entire regime and may include, for instance, certain techniques for law enforcement that human rights advocates object to in principle, but are effectively restrained by limitations on their scope and use.
>
> Transparency aims at keeping governments accountable with regard to the use of the techniques and acts as a safeguard regarding the authorization of techniques within the legal framework. Transparency further informs the public about consequences and their risks as a result of trade-offs. Trade-offs manifest in the digital realm, such as weakened security because of design mandates, or in the physical world, such as lessened public safety (e.g., use of encrypted communication by criminal and terrorist organizations). Such drawbacks, however, can be offset partially with other measures.

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). These improvements include:

- **Capability and Capacity:** Train and build up capabilities for law enforcement and the judiciary to conduct their mission in the digital age. Invest in and strengthen digital forensics and decryption, circumvention capabilities and capacities for law enforcement and establish effective mechanisms for resource coordination and pooling among national and local law enforcement authorities. Further enhance the ability of law enforcement and the judiciary to make informed decisions about cyber-enabled cases and handle digital evidence.[109] Provide support mechanisms for technically less advanced law enforcement and judicial entities.
- **Mutual Legal Assistance and Cross-Border Cooperation:** Improve the MLAT process to make it more effective, particularly for urgent requests to transfer data.[110] Work towards establishing bilateral and multilateral agreements with key partners to address cross-jurisdictional issues for agreed upon scenarios (e.g., access to cloud storage in foreign jurisdictions),[111] resolve common conflicting cross-jurisdictional issues (including conflicting data protection provisions) and the handling of digital evidence.[112] Work towards cross-border cooperation among law enforcement authorities to combat cyber-enabled crime and terrorism which is often committed in and from multiple jurisdictions. Agree on scenarios and procedures for cross-border cooperation (e.g., relating to compelled provider assistance and lawful hacking). Improve international law enforcement cooperation by developing expert communities, sharing best practices and establishing points of contact among law enforcement authorities.
- **Public-Private Cooperation:** The private sector, particularly the ICT industry and academia, should continue to support law enforcement in identifying and develop-

[109] E.g., educate the judiciary about ICT and cyber risk to make informed decisions when authorizing certain actions, such as lawful hacking in a particular case.

[110] Woods; Richard Clarke and others, Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, 2013 <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>.

[111] Bilateral agreements may provide a cornerstone for future multilateral agreements that address pressing issues on a regional or global level.

[112] See, the 2017 EU consultation on cross-border access to digital evidence: European Commission, 'Public Consultation on Improving Cross-Border Access to Electronic Evidence in Criminal Matters', 2017 <https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en>.

ing innovative approaches to enhance law enforcement's ability to detect, prevent and investigate cyber-enabled crime and terrorism. Law enforcement should establish close, trusted working relationships with key service providers, product and device manufacturers, ICT firms and Internet service providers (ISPs).

- **Collaboration:** Governments should collaborate to ensure consistency of their legal frameworks internationally so that businesses operating across the borders are not put into unavoidable situations of incompliance due to conflicts of laws and regulatory regimes.
- **Alternative Approaches:** Invest in alternative ICT-enabled approaches (e.g., analysis of communications metadata, use of new data sources from the Internet of Things and smart home devices or machine-to-machine communications), traditional law enforcement methods and workarounds for encryption (e.g., by guessing or deriving a password, discovering login details as part of a physical search or locating a plaintext copy of the data).[113] Train law enforcement and raise awareness about unused or underutilized data held by private sector entities that are useful for investigative and/or preventive law enforcement purposes. Build tools and platforms that securely provide access to such data under the respective legal authorities and limitations.
- **Privacy and Other Human Rights:** Ensure that new technical measures and organizational arrangements are subject to stringent legal limitations and judicial and technical oversight in order to protect human rights. Any measures need to follow the guiding principles of proportionality, necessity and legality.
- **Technical and Operational Standardization:** Work towards standardization of technical and operational aspects of approaches on an international level to help companies better protect consumer data and reduce their compliance cost, particularly for entities operating in and subject to multiple jurisdictions.[114]
- **Measurement:** Establish shared definitions of the problem and measure the impact of encryption on the law enforcement mission. Collect and analyze data.

EWI Commentary: Infrastructure improvements address a host of technical, organizational and legal issues that are not about encryption per se but provide law enforcement and the judiciary with the necessary means to operate effectively in the digital environment. These measures could lower the perceived impact encryption has on law enforcement's access to data. For instance, MLAT and cross-border collaboration issues are often not about encryption, but a prerequisite to deal with crime and terrorist cases that involve multiple jurisdictions, and have been a hindrance for investigations and prosecutions. As countries are expanding their jurisdictions (e.g., directly requesting access to data in foreign jurisdictions and expanding jurisdiction over personal data), occurrences of cross-jurisdictional conflicts are likely to increase. Attempts to streamline cross-jurisdictional issues must consider human rights implications in cases where counterparts follow lower human rights standards. Harmonization of technical and operational standards for techniques (e.g., communications intercept) will further support law enforcement cooperation but also help protect consumer data and ease the burden of compliance for companies subject to multiple jurisdictions and national requirements. Furthermore, such corporations are often confronted with conflicting legal requirements from different jurisdictions (e.g., lawful request to provide data to authorities in one jurisdiction when the same data is protected under statutes of another jurisdiction). Governments need to collaborate to avoid irreconcilable patchworks of rules and laws for the reasons outlined above, but also to avoid the fragmenting effects these conflicting laws have on the Internet. For new capabilities, particularly forensic and decryption capabilities as well as alternative approaches, a clear scope and limitations need to be established to ensure that they are used in a necessary and proportionate fashion. The infrastructure improvements are balanced if they are narrowly tailored and aimed at fighting crime and terrorism. Infrastructure improvements require significant political will and resource investments to go forward.

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, and must not open the doors for wide-ranging changes that affect entire classes of users, services or devices. Compelled assistance should be the preferred technique to facilitate lawful access to third-party encryption products, services and ephemeral communications; before other, more intrusive techniques are employed. Compelled assistance should avoid measures that undermine security or trust of broad categories of users (e.g., compelling a provider to commit surreptitious updates).

EWI Commentary: Compelled assistance is a central part of most regimes to gain access to data. Law enforcement authorities rely significantly on private

[113] Kerr and Schneier.

[114] Note the distinction between technical/operational harmonization and value harmonization. Technical/operational standardization allows for companies to better protect consumer data and reduce compliance cost but does not imply value harmonization. States will have separate legal requirements, yet technical/operational aspects should be standardized.

sector entities to achieve access. As some service providers and device manufacturers have recently not only advanced the wide adoption of encryption, prominently through ubiquitous device encryption, but also relinquished their ability to produce a decryption key and provide access to decrypted data, gaining access through compelled provider assistance has proven increasingly difficult and in some cases of limited use. The report recognizes the difficulties that law enforcement authorities face with regard to access to encrypted data on smart phones and over-the-top encrypted or ephemeral messaging services, including cases where the compelled entity is extraterritorial or is diffuse, such as the open source community. Yet, there are a variety of products and services that remain accessible via compelled provider assistance as they were designed to comprise access recovery mechanisms for business purposes.[115]

Clear rules define where and to what extent compelled provider assistance is applicable under the legal framework. A rule, for instance, may state that law enforcement must have the physical device in possession in order to request technical assistance; another rule might require that technical assistance be limited to particular, individual cases. Such measures help limit risks and avoid broad application of access solutions developed through technical assistance. Moreover, clear rules help to avoid unintended, possibly ex-ante, architectural changes to a system in order comply with future requests for technical assistance. Similarly, the inability to produce decrypted data under a compelled provider assistance request should not result in severe criminal or financial sanctions that would inhibit innovation or undermine cybersecurity in unintended ways.

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, and 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. Enhanced digital forensic capabilities for accessing devices in the local possession of law enforcement must be emphasized over remote lawful hacking that targets data on end points or data streams passing through intermediary infrastructure. Lawful hacking should be accompanied with investments in enhanced digital forensic capabilities. Governments should not employ surreptitious updates via lawful hacking (i.e., broken key signing mechanism, controlled by the state) and should avoid surreptitious updates via compelled provider assistance (i.e., key signing mechanism remains intact, administered by the provider), except for extraordinary circumstances in a subset of cases as defined by law. As a norm, the application of lawful hacking with targets in foreign jurisdictions or of unknown locations should be narrowly restricted and only be conducted in close collaboration with the respective foreign authorities. Due to human rights concerns, government should establish controls concerning the export of law enforcement investigative tools for online surveillance and communications interception.

EWI Commentary: Lawful hacking has become a critical technique for circumventing encryption in the context of criminal investigations (e.g., investigating cyber-enabled organized crime by exploiting vulnerabilities in messaging services to gain access to protected communications). The reasons for the recommended limitations of lawful hacking are the significant harmful effects it may cause.[116] Such operations can have unintended effects or go awry, resulting in decreasing the security of non-targeted systems and users and leave them vulnerable. Targeting (perhaps unknowingly) systems in foreign jurisdictions can result in diplomatic tensions. But also, such tools are subject to unauthorized use, or can be lost or stolen and subsequently used by criminals or terrorists. Lawful hacking, particularly surreptitious updates, has the potential to undermine users trust in a key cybersecurity approach. Users may disable automated update mechanisms en masse "to keep safe from government interference," with tremendous consequences for the security of the ecosystem. Lawful hacking remains expensive and is thus affordable to well-resourced law enforcement entities only. To strike a balance in the use of lawful hacking in an encryption policy regime, the approach needs to be embedded in a legal framework with strict authorizations and limitations for extraordinary rather than common use.

[115] Also, note that other types of data and evidence are relevant in criminal investigations and prosecutions that are not inaccessible due to encryption. Financial institutions, for instance, provide banking information upon lawful request, without the need for law enforcement access to transactional banking systems to collect evidence.

[116] Minimum standards for lawful hacking are currently being developed by a transatlantic expert working group. Transatlantic Cyber Forum, Policy Track #1: Encryption Policy & Government Hacking, <https://www.stiftung-nv.de/en/project/international-cyber-security-policy#erstens>.

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. Technical protections should minimize the effects of design mandates on cybersecurity and costs for system changes should be borne by the regulating entity. Where possible, design mandates should make use of existing systems functions to fulfil the requirement and avoid in-depth architectural changes to the service or products.

> EWI Commentary: Design mandates provide a policy option to require service providers and device manufacturers to retain the ability to gain access to encrypted data that might otherwise be inaccessible without such a mandate. However, due to negative effects that design mandates can have on cybersecurity and their expansive implementation costs, design mandates should be limited in scope and function. Limitations can come in the form of particular designated services and products (e.g., end devices, communication services and cloud services) that are determined through public regulatory procedures. Being subject to annual recertification and risk assessment help to minimize overall risk of such design mandates to cybersecurity and help balance the overall encryption policy regime. In some cases, current business models include access recovery functions (e.g., key recovery for cloud service accounts) which provide a sufficient technical access for lawful requests and hence would not be subject to additional access requirements. Requesting access to data from a product or service that is subject to a design mandate would be subject to the same stringent judicial oversight requirements as compelled assistance.

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. Vulnerabilities temporarily kept undisclosed should be subject to periodic reevaluation. The VEP should sufficiently address safeguards to protect vulnerabilities from loss or theft and be applicable to third parties that report vulnerabilities to law enforcement.

> EWI Commentary: The government's decision to disclose or keep concealed a software or hardware vulnerability for law enforcement purposes must be based on comprehensive, transparent vulnerability management that includes a transparent vulnerabilities equities process that reflects when governments bear responsibility to disclose and strengthen overall cybersecurity.[117] Once a vulnerability is determined for public disclosure, the objective is to inform the service provider or device manufacturer in order to promptly fix the vulnerability. A vulnerability disclosure requirement with limited exceptions for non-disclosure (including limitations on third-party non-disclosure agreements), is an effective means to limit and balance lawful hacking as a technique. Comprehensive vulnerability management with a transparent vulnerabilities equities process strengthens trust among law enforcement, the ICT industry and users, if appropriately enacted in law to ensure compliance, independent oversight and a public summary reporting to the legislature. Rather than insisting on strict, uniform disclosure timelines for all types of vulnerabilities, the emphasis should be on the overall vulnerability management and a timely disclosure process once a vulnerability has been determined for public disclosure. Disclosure of vulnerabilities may have a cumulative, disruptive effect on the vulnerability market and law enforcement's ability to acquire them might be subsequently constrained; however, this is a subservient consideration and strengthens the overall notion that lawful hacking must be limited in it application. Note that the report recognizes that the government's approach to vulnerability disclosure goes beyond the needs of law enforcement and is influenced by other considerations not addressed here, including the use of vulnerabilities for national security purposes in the intelligence and military realm (e.g., cyber weapons).

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. Governments must not require decryption keys be stored with local authorities.

> EWI Commentary: While data localization requirements are most often discussed in the context of national security in order to locate sensitive data within one's own jurisdiction, data localization also provides some

[117] Rob Joyce, 'Improving and Making the Vulnerability Equities Process Transparent Is the Right Thing to Do', The White House, 2017 <https://www.whitehouse.gov/blog/2017/11/15/improving-and-making-vulnerability-equities-process-transparent-right-thing-do>.

advantages for law enforcement.[118] If data is stored locally, requesting lawful access is comparatively simpler than when the same data would reside in a foreign jurisdiction, in which case a request through the burdensome MLAT process becomes unavoidable. Businesses subject to such requirements purport however, that data localization may limit service functionality due to local restrictions and subsequently reduce the value of modern ICT systems. As data localization arguably comes with significant ICT costs, service providers comply, in many cases, to gain market access. It seems likely that such costs depend heavily on the market size (e.g., low cost per user in a large market such as the EU) and companies may have already incurred design costs in their decision to enter a market. Data localization may also create significant non-tariff trade barriers and negatively affect data flows, undercut information security (e.g., if the law requires the storage of decryption keys with local security authorities) and undermine innovation.

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. The review should consider the effectiveness and usefulness of the techniques and limitations in the regime and warrant adjustments based on altered risk calculations. Independent experts (e.g., an expert group or standing commission) should provide policymakers with state-of-the art technical, legal and risk assessments and provide recommendations for adjustments in anticipation of short and long-term developments, where needed. To elevate the public discussion and allow for a thorough assessment of proposed policies, proposals for change should be accompanied by technical blueprints, feasibility studies and risk/impact assessments.

EWI Commentary: A periodic review that includes the private sector and civil society allows for systematic evaluation of the effects of different trade-offs over time and ensures that the balances in the regime are maintained and if necessary are adjusted. It further allows to make adjustments to the regime based on technical developments or innovations as well as to respond to changes in crimes being conducted. For example, the advent of usable quantum computing, as is expected in the next 10 to 20 years, could radically alter the encryption landscape, but also more mundane developments such as an increase of encryption by organized crime may trigger changes to the regime balance.

[118] E.g., data localization requirements for government entities may require sensitive, national security data or citizens' personally identifiable information (PII) not to be stored in foreign countries.

7 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.

8 References

18 U.S. Code § 2515 - Prohibition of Use as Evidence of Intercepted Wire or Oral Communications <https://www.law.cornell.edu/uscode/text/18/2515>

18 U.S. Code § 2516 - Authorization for Interception of Wire, Oral, or Electronic Communications <https://www.law.cornell.edu/uscode/text/18/2516>

18 U.S. Code § 2518 - Procedure for Interception of Wire, Oral, or Electronic Communications <https://www.law.cornell.edu/uscode/text/18/2518>

47 U.S. Code § 1008 - Payment of Costs of Telecommunications Carriers to Comply with Capability Requirements <https://www.law.cornell.edu/uscode/text/47/1008>

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, 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>

Bedell, Zoe, and Benjamin Wittes, 'Civil Liability for End-to-End Encryption: Threat or Fantasy? Part I', Lawfare Blog, 2015 <https://www.lawfareblog.com/civil-liability-end-end-encryption-threat-or-fantasy-part-i>

Clarke, Richard, Michael Morell, Geoffrey Stone, Cass Sunstein, and Peter Swire, Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, 2013 <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>

Clement, Andrew, and Jonathan Obar, 'Keeping Internet Users in the Know or in the Dark: An Analysis of the Data Privacy Transparency of Canadian Internet Carriers', Journal of Information Policy, 6 (2016), 294–331 <http://www.jstor.org/stable/10.5325/jinfopoli.6.2016.0294>

Council of the European Union, 'Council Conclusions of 20 November 2017 on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU', 2017 <http://www.consilium.europa.eu/media/31666/st14435en17.pdf>

Court of Justice of the European Union, Judgement of the Court (Grand Chamber), 6 October 2015 <http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=116845>

Dutch Ministry of Security and Justice, Cabinet's View on Encryption, 2016 <https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on-encryption>

ENISA, 'The Netherlands: Cabinet Launched Position on Encryption', ENISA, 21 April 2016 <https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/the-netherlands-cabinet-launched-position-on-encryption>

European Commission, '2017 Eleventh Progress Report towards an Effective and Genuine Security Union', 2017 <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf>

———, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC) (Brussels, 2011) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF>

———, 'Public Consultation on Improving Cross-Border Access to Electronic Evidence in Criminal Matters', 2017 <https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en>

Figliola, Patricia Moloney, Digital Surveillance: The Communications Assistance for Law Enforcement Act (Washington, D.C., 2007) <https://fas.org/sgp/crs/intel/RL30677.pdf>

Freedom House, 'Freedom House's Annual Freedom in the World and Freedom on the Net Reports on the Global Development of Political, Civil, and Digital Rights', Freedom on the Net 2017, 2017 <https://freedomhouse.org/reports>

Gidari, Albert, 'Wiretap Reports Not So Transparent', The Center for Internet and Society, 2017 <http://cyberlaw.stanford.edu/blog/2017/01/wiretap-reports-not-so-transparent>

Goodin, Dan, 'Anatomy of a Hack: How Crackers Ransack Passwords like "qeadzcwrsfxv1331"', Ars Technica, 27 May 2013 <https://arstechnica.com/information-technology/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/2/>

Greenberg, Andy, 'These Are The Prices AT&T, Verizon and Sprint Charge For Cellphone Wiretaps', Forbes, 3 April 2012 <https://www.forbes.com/sites/andygreenberg/2012/04/03/these-are-the-prices-att-verizon-and-sprint-charge-for-cellphone-wiretaps>

Group-IB, Lazarus Arisen: Architecture, Techniques and Attribution, 2017 <https://www.group-ib.com/resources/threat-research/lazarus.html>

Hern, Alex, 'WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017', The Guardian, 30 December 2017 <https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware>

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>

IX Maps, 'Glossary' <https://www.ixmaps.ca/learn/glossary.php>

Joyce, Rob, 'Improving and Making the Vulnerability Equities Process Transparent Is the Right Thing to Do', The White House, 2017 <https://www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/>

Kaye, David, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Human Rights Council, A/HRC/29/32, 22 May 2015 <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc>

Kerr, Orin, and Bruce Schneier, Encryption Workarounds, Georgetown Law Journal, 2017 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033>

Koebler, Jason, 'Senator: Crime Victims Should Be Able to Sue Apple, Google for Encrypting Data', Motherboard, 8 July 2015 <https://motherboard.vice.com/en_us/article/ezvw9z/senator-crime-victims-should-be-able-to-sue-apple-google-for-encrypting-data>

Kris, David, 'U.S. Government Presents Draft Legislation for Cross-Border Data Requests', Lawfare Blog, 2016 <https://www.lawfareblog.com/us-government-presents-draft-legislation-cross-border-data-requests>

La Rue, Frank, 'The 2011 Report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression Expressed Concerns about Nation States' Actions against and Justification for the Interference with Individuals' Online Communic', Human Rights Council, 2011 <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>

———, 'UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', United Nations Human Rights Council, 2013 <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>

Lin, Tiffany, and Mailyn Fidler, 'Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement', Berkman Klein Center, 2017 <https://cyber.harvard.edu/publications/2017/09/berklett>

Mayer, Jonathan, Government Hacking, Yale Law Journal, 2018 <https://www.yalelawjournal.org/pdf/Mayer_k3iy4nv8.pdf>

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>

Nelson, Steven, 'Cell Providers Collect Millions From Police for Handing Over User Information', U.S. News and World Report, 9 December 2013 <https://www.usnews.com/news/articles/2013/12/09/cell-providers-collect-millions-from-police-for-handing-over-user-information>

New York County District Attorney, Smartphone Encryption and Public Safety (New York, NY, 2017) <http://manhattanda.org/sites/default/files/2017 Report of the Manhattan District Attorney's Office on Smartphone Encryption.pdf>

OECD, Recommendation of the Council Concerning Guidelines for Cryptography Policy, 1997 <http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=115&InstrumentPID=111&Lang=en&Book=False>

Olsen, Matt, 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>

OWASP, 'Guide to Cryptography' <https://www.owasp.org/index.php/Guide_to_Cryptography#Cryptographic_Functions>

Privacy International, 'Government Hacking and Surveillance: 10 Necessary Safeguards', 2017 <https://privacyinternational.org/node/957>

Rozenshtein, Alan, 'Surveillance Intermediaries', 2007 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2935321>

Schneier, Bruce, Kathleen Seidel, and Saranya Vijayakumar, 'A Worldwide Survey of Encryption Products', 2016 <https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf>

Schulz, Wolfgang, and Joris van Hoboken, 'Human Rights and Encryption', UNESCO Series on Internet Freedom, 2016 <http://unesdoc.unesco.org/images/0024/002465/246527E.pdf>

Shackleford, Dave, 'Regulations and Standards: Where Encryption Applies', SANS Institute, 2007 <https://www.sans.org/reading-room/whitepapers/analyst/regulations-standards-encryption-applies-34675>

Thompson II, Richard M., and Chris Jaikaran, Encryption: Selected Legal Issues (Washington, D.C., 2016) <https://fas.org/sgp/crs/misc/R44407.pdf>

Turoff, Murray, 'The Policy Delphi', in The Delphi Method: Techniques and Applications, ed. by Harold A. Linstone and Murray Turoff, 2002, pp. 80–96

U.S. Department of Justice, The Implementation of the Communications Assistance for Law Enforcement Act, 2006 <https://oig.justice.gov/reports/FBI/a0613/findings.htm>

U.S. House Judiciary Committee and the House Energy and Commerce Committee, 'Encryption Working Group Year-End Report' (Washington, D.C.: Encryption Working Group, 2016) <https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf>

UN Human Rights Committee, 'UN Human Rights Committee, General Comment on Freedom of Opinion and Expression', CCPR/C/GC/34, 2011 <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>

UN Office of the High Commissioner, 'Report on Encryption, Anonymity, and the Human Rights Framework', 2017 <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>

United States Courts, Wiretap Reports, 2016 <http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports>

The White House, Executive Order -- Blocking the Property and Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology, The White House Archives, 2012 <https://obamawhitehouse.archives.gov/the-press-office/2012/04/23/executive-order-blocking-property-and-suspending-entry-united-states-cer>

———, Vulnerabilities Equities Policy and Process for the United States Government (Washington, D.C., 2017) <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>

Woods, Andrew, Data Beyond Borders: Mutual Legal Assistance in the Internet Age, 2015 <https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf>

9 Appendix: Analysis of the Expert Consultation

Draft policy regimes were evaluated by experts in a consultation following the process outlined in this report. Section 5 describes two proposed regimes that originated from the draft regimes and have been modified based on the issues the experts raised.[119] This appendix attempts to summarize the more than 200 pages of comments EWI received. This summary cannot reproduce the nuanced views expressed. Moreover, there were disagreements among experts on important points of policy.

From the outset, the draft regimes relied significantly on compelled provider assistance as a key policy approach to facilitate law enforcement access to encrypted data in plaintext, as opposed to more extreme policy approaches that would ban or limit encryption altogether. The two draft regimes differed in that draft Regime 1 employed lawful hacking as a critical component, whereas draft Regime 2 emphasized design mandates, but no lawful hacking. These distinctions carried over into the proposed regimes in Section 5.

Despite the differences, experts considered both proposed regimes as generally useful and effective for law enforcement. Compelled provider assistance and measures to improve cross-jurisdiction cooperation and cross-border access to data and evidence were considered very relevant components in both regimes.[120] In addition, providing local enhanced forensic and decryption capabilities was assessed as particularly useful with little downsides to society (i.e., to deploy forensic capabilities on a protected smart phone that law enforcement has in its physical possession), and thus included in both regimes as a systemic improvement.[121]

Experts noted the downsides that come with lawful hacking and design mandates for encrypted data on smart phones, encrypted messaging services and ephemeral communications. They indicated the international effects of both regimes as positive, as the experts recognized the importance of international cooperation and exchange of case-relevant information and evidence in combating cyber-enabled crime and terrorism. Thus, both regimes include the development of bilateral agreements towards due process equivalence and the strengthening of reciprocal access in foreign jurisdiction under MLATs as systemic improvements. A few experts cautioned against information sharing with jurisdictions that adhere to lesser protection standards of human rights, and also pointed out that in cross-border cases, facilitated by MLAT or bilateral agreements, decryption keys must not be subject to general sharing of data or digital evidence. Further, both regimes propose to conduct capacity building for law enforcement to handle encrypted and

[119] See section 4.4 for background on the expert consultation process.

[120] Note that cross-jurisdictional access or exchange of information (e.g., under MLAT) is a more general lawful access issues, and less of an encryption concern. Similarly, whether a state considers particular actors "dissidents," "terrorists" or "freedom fighters" is also not about encryption.

[121] OTT services are third-party services built on top of an infrastructure or network with which they often compete. For example, WhatsApp uses a mobile phone platform to offer communication services through the infrastructure provided by a telecommunications operator with which it competes in the communication services market.

unencrypted data, and enhance cooperation between the private sector and law enforcement and among law enforcement entities internationally, which were strongly supported by the experts.

Considering the entirety of the regime (as opposed to individual techniques and limitations under the regime), particular concerns were expressed as to negative effects of both proposed regimes on cybersecurity and the ICT market and business. Experts indicated a lower level of confidence in accurately estimating cost implications of both regimes and argued the need for additional information and analysis about the technical infrastructure and systems architecture. Some estimates indicated significantly higher overall costs for both regimes, while others concluded that additional costs from the status quo, if any, were minimal or negligible due to the government's cost reimbursement (covering infrastructure updates and per-use fee) and the similarities of the regimes (particularly Regime 1) with current policies in some Western governments. Yet, one expert pointed out that hidden costs are notoriously difficult to account for and may not be recoverable under the proposed provision. The expert consultation showed that assessing costs is particularly difficult. An in-depth study of the cost of different policy options would be very useful for the encryption policy debate. With regard to human rights, assuming that these proposed regimes would be applied under a regime that constitutionally ensures the rule of law and protects human rights, experts considered the limitations (e.g., judicial authorities, public summary reporting) in the proposed regimes overall to be effective and sufficient to protect human rights.

Compelled provider assistance was recognized in both proposed regimes as a key element in facilitating access to encrypted data and communications. However, experts differed in their understanding as to what degree compelled provider assistance would force companies (e.g., software vendors, device manufacturers) to provide case-by-case technical assistance to help write software that circumvents protections in a particular case and to what degree it would restrict the freedom of companies to innovate and enact the best security measures in anticipation of future requests for assistance. This assessment reflects legal uncertainties regarding compelled provider assistance present in the current debates (e.g., in the FBI vs. Apple case that tried to test these grounds, the FBI withdrew the legal case before it could be settled as eventually access to the data was facilitated by a third party, not the device manufacturer).

The experts weighed in on lawful hacking as an option to address third party (over-the-top) encrypted messaging and ephemeral communication services. Experts noted that while lawful hacking can be a useful tool, it remains an expensive option with potential negative cybersecurity implications, does not scale and is not available to most law enforcement authorities. One expert noted that lawful hacking tools could be stolen or lost. Among the group of experts, there were diverging views on the implications of vulnerability disclosure as a way to minimize negative impacts of lawful hacking on overall cybersecurity and extensive use by law enforcement. Many experts pointed out, however, that a too strict and short disclosure timeline might affect the vulnerability market and subsequently inhibit law enforcement from effectively using this increasingly important tool. As an extension of lawful hacking, experts commented on surreptitious updates as a law enforcement tool. Industry representatives, in particular, pointed out that surreptitious updates should not be pursued as it would require law enforcement to somehow acquire and compromise the signing key to conduct these updates without the help of the software vendor. Several experts voiced strong opposition to this approach arguing it would undermine user trust in security updates which is a key tool to provide the entire cyber ecosystem with security updates to protect their systems. Views diverged on whether software vendors could be forced under compelled provider assistance to deliver targeted software updates to computers and users as part of a lawful investigation. In both cases, experts argued, as a consequence, users may turn off the update mechanism for critical security updates to avoid government interference with their systems, and at the same time opening the door to become vulnerable to unpatched vulnerabilities, as such this could have significant impact on the overall security of the entire ICT ecosystem.

The assessment of design mandates (e.g., mandatory key recovery) in proposed Regime 2 was not unanimously negative. Several experts saw it as a useful technique to gain access to data, particularly when it already existed and was implemented for other business practices and would only need to be repurposed (e.g., key recovery in cloud storage is common business practice to ensure a user or customer can regain access if a password is lost). Yet, some experts strongly rejected such approaches as a policy option; they were of the view that such design mandates can effectively be undermined by adding another layer of encryption (e.g., encrypt files before uploading to a cloud storage services that is subject to a design mandate), rendering the approach ineffective. In particular, many experts rejected mandatory key recovery mechanisms for cloud storage or encrypted data on smart phones; yet, others argued that such risk is acceptable, particularly if the underlying mechanisms that would enable third-party access already exist. Here, costs were also a concern. Some experts noted the potential negative effect on industry competitiveness: a mandatory technical access requirement in form of a design mandate, they argued, would impair the competitiveness of ICT firms that must comply with the design mandate or at least make it costly to maintain separate versions of services and products destined for foreign markets. With regard to design mandates, one expert noted the possibility to link design mandates with lawful hacking and vulnerability disclosure. Under such an arrangement, if a specific provider agrees to implement design mandates, authorities would agree not to deploy lawful hacking against the provider and to disclose vulnerabilities they become aware of immediately. If a provider, however, does not agree, it could be subject to lawful hacking in a criminal case—if other options of lawful access are exhausted—and vulnerability disclosure would be delayed. This would take into account the fact that in reality it would not be possible to ensure that design mandates are followed by everyone (at the minimum because of the jurisdictional issues) and this would give incentive to providers to self-comply. We did not propose this idea in order to retain a clear distinction between the two alternative approaches.

As part of identifying trade-offs during the regime adoption process, experts discussed what benefits for law enforcement afforded by some approaches were—in some cases by far—outweighed by their negative consequences for cybersecurity, national security, commerce and human rights. A common argument in assessing trade-offs was that a measure (applicable to all users) does not present an acceptable risk (for all users), if it can be circumvented relatively easily and thus, rendered ineffective by a single user (e.g., criminals apply an additional layer of encryption). Yet, other experts opposed that view, arguing that while techniques might be circumvented in a particular instance, that does not necessarily render the method overall ineffective or useless for law enforcement access purposes. Some measures, such as data localization for easier, domestic law enforcement access, were rejected because similar outcomes can be achieved with other, less costly means. To gain an overall balanced regime, such measures were excluded from the proposed regimes.

The regimes attempt to provide pathways for law enforcement to access encrypted data in plaintext, but take into account that this will not always be successful, even in cases where a court authorized such access (e.g., warrant). This is a consequence of the trade-offs and balancing of multiple interests and values. As with finding a balance or a compromise, no party will achieve all its goals (e.g., law enforcement will not be able to get access to all encrypted phones). In a regime that employs design mandates and requires key escrow, there is always a possibility someone would use third-party encryption, even if this is outright banned or subject to severe sanctions. There is no absolute access here, just as there is no absolute security. Gaining access to data—in the end—depends on time and resources. Lawful hacking might be a tool—in combination with compelled provider assistance—that can effectively force access to encrypted data on smart phones, encrypted third-party messaging or ephemeral communication services. For instance, in Regime 1, a combination of lawful hacking and compelled provider assistance, plus some form of traditional law enforcement work, might prove effective to combat cyber-enabled criminals who protect their communications with encryption. Alternatively, enhanced digital forensic capabilities can provide access to encrypted data in some, but not all, cases. In Germany and France forensic and decryption capabilities are part of the national strategy enabling lawful access to encrypted data. In addition, several approaches can be combined in a regime—including compelled provider assistance, lawful hacking and enhanced forensic capabilities which is what Regime 1 proposes as an approach.

Board of Directors

OFFICE OF THE CHAIRMAN

Ross Perot, Jr. (U.S.)
Chairman
EastWest Institute
Chairman
Hillwood Development Co. LLC

H.E. Dr. Armen Sarkissian (Armenia)
Vice Chairman
EastWest Institute
President
Eurasia House International
Ambassador Extraordinary and Plenipotentiary
Embassy of the Republic of Armenia to the United Kingdom
Former Prime Minister of Armenia

R. William Ide III (U.S.)
Counsel and Secretary
Chair of the Executive Committee
EastWest Institute
Partner
Dentons US LLP

Amb. Cameron Munter (U.S.)
CEO and President
EastWest Institute
Former Ambassador
Embassy of the United States to Pakistan

CO-FOUNDERS

John Edwin Mroz* (U.S.)
Former President and CEO
EastWest Institute

Ira D. Wallach* (U.S.)
Former Chairman
Central National-Gottesman Inc.

MEMBERS

Peter Altabef (U.S.)
President and CEO
Unisys

Hamid Ansari (U.S.)
President and Co-Founder
Prodea Systems, Inc.

Tewodros Ashenafi (Ethiopia)
Chairman and CEO
Southwest Energy (HK) Ltd.

Mary McInnis Boies (U.S.)
Counsel
Boies, Schiller & Flexner LLP

Sir Peter Bonfield (UK)
Chairman
NXP Semiconductors

Matt Bross (U.S.)
Chairman and CEO
Compass-EOS

Robert N. Campbell III (U.S.)
Founder and CEO
Campbell Global Services LLC

Maria Livanos Cattaui (Switzerland)
Former Secretary-General
International Chamber of Commerce

Michael Chertoff (U.S.)
Executive Chairman and Co-Founder
The Chertoff Group
Former Secretary of the U.S. Department of Homeland Security

David Cohen (Israel)
Chairman
F&C REIT Property Management

Joel H. Cowan (U.S.)
Professor
Georgia Institute of Technology

Addison Fischer (U.S.)
Chairman and Co-Founder
Planet Heritage Foundation

Stephen B. Heintz (U.S.)
President
Rockefeller Brothers Fund

Hon. Steven S. Honigman (U.S.)
Counselor
Information and Infrastructure Technologies, Inc.

Dr. Hu Yuandong (China)
Chief Representative
UNIDO ITPO-China

John Hurley (U.S.)
Managing Partner
Cavalry Asset Management

Amb. Wolfgang Ischinger (Germany)
Chairman
Munich Security Conference

Ralph Isham (U.S.)
Managing Director
GH Venture Partners LLC

Anurag Jain (U.S.)
Chairman
Access Healthcare

Gen. (ret) James L. Jones (U.S.)
Former U.S. National Security Advisor
Former Supreme Allied Commander Europe
Former Commandant of the Marine Corps

George Kadifa (U.S.)
Managing Director
Sumeru Equity Partners

Haifa al Kaylani (Lebanon/Jordan)
Founder and Chairperson
Arab International Women's Forum

Sezgin Baran Korkmaz (Turkey)
CEO
SBK Holding

Zuhal Kurt (Turkey)
Chairman of the Board
Kurt Group

Gen. (ret) T. Michael Moseley (U.S.)
President and CEO
Moseley and Associates, LLC
Former Chief of Staff
United States Air Force

Karen Linehan Mroz (U.S.)
President
Roscommon Group Associates

F. Francis Najafi (U.S.)
CEO
Pivotal Group

Amb. Tsuneo Nishida (Japan)
Professor
The Institute for Peace Science at
Hiroshima University
Former Permanent Representative of
Japan to the United Nations

Admiral (ret)
William A. Owens (U.S.)
Chairman
Red Bison Advisory Group LLC
Chairman of the Board of Directors
CenturyLink

Sarah Perot (U.S.)
Director and Co-Chair for Development
Dallas Center for Performing Arts

Laurent M. Roux (U.S.)
Founder and President
Gallatin Wealth Management, LLC

Mike Sarimsakci (Turkey)
Founder and President Partner
Alterra International, LLC

Ikram ul-Majeed Sehgal
(Pakistan)
Chairman
Security & Management Services Ltd.

Amb. Kanwal Sibal (India)
Former Foreign Secretary of India

Kevin Taweel (U.S.)
Chairman
Asurion

Alexander Voloshin (Russia)
Chairman of the Board
JSC Freight One (PGK)
Non-Executive Director
Yandex Company

Amb. Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Hilton Smith, Jr. (U.S.)
President and CEO
East Bay Co., LTD

CHAIRMEN EMERITI

Martti Ahtisaari (Finland)
Former Chairman
EastWest Institute
2008 Nobel Peace Prize Laureate
Former President of Finland

Berthold Beitz* (Germany)
President
Alfried Krupp von Bohlen und
Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California, Los Angeles

Francis Finlay (UK)
Former Chairman
Clay Finlay LLC

Hans-Dietrich Genscher* (Germany)
Former Vice Chancellor and Minister of
Foreign Affairs of Germany

Donald M. Kendall (U.S.)
Former Chairman and CEO
PepsiCo Inc.

Whitney MacMillan (U.S.)
Former Chairman and CEO
Cargill Inc.

Mark Maletz (U.S.)
Former Chairman, Executive Committee
EastWest Institute
Senior Fellow
Harvard Business School

George F. Russell, Jr. (U.S.)
Former Chairman
EastWest Institute
Chairman Emeritus
Russell Investment Group
Founder
Russell 20-20

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
CEO
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
President
Institute for Regional Cooperation and
Conflict Prevention (INCOR)
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

John W. Kluge* (U.S.)
Former Chairman of the Board
Metromedia International Group

Amb. Maria-Pia Kothbauer
(Liechtenstein)
Ambassador of Liechtenstein to Austria,
the OSCE and the United Nations in Vienna

William E. Murray* (U.S.)
Former Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates Inc.

Leo Schenker (U.S.)
Former Senior Executive Vice President
Central National-Gottesman Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg (Norway)
President
Norwegian Red Cross

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead* (U.S.)
Former Co-Chairman
Goldman Sachs
Former U.S. Deputy
Secretary of State

* Deceased

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

EastWest
INSTITUTE

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