Confronting Wicked Crypto

Wicked Problems, Encryption Policy, and Exceptional Access Technology

Kevin Nicholas Kredit

A Thesis Submitted to the Graduate Faculty of

GRAND VALLEY STATE UNIVERSITY

In

Partial Fulfillment of the Requirements

For the Degree of

Master of Science

Applied Computer Science

December 2020

Dedication

For Kristen.

Abstract

Public debate has resumed on the topic of exceptional access (EA), which refers to alternative means of decryption intended for law enforcement use. The resumption of this debate is not a renege on a resolute promise made at the end of the 1990s "crypto war"; rather, it represents a valid reassessment of optimal policy in light of changing circumstances. The imbalance between privacy, access, and security in the context of constantly changing society and technology is a wicked problem that has and will continue to evade a permanent solution. As policymakers consider next steps, it is necessary that the technical community remain engaged. Although any EA framework would increase risk, the magnitude of that increase varies greatly with the quality of the technical and regulatory approach. Furthermore, if one considers hard-line legislative action and malicious abuse of cryptosystems as part of the threat model, well-designed EA may reduce risk overall.

The root of the conflict lies in cryptography's dual role as an enabler of unprecedented privacy and a cornerstone of security. The emergence of strong encryption incited the first crypto war, and its proliferation is causing the second. In response to both polarized and conciliatory voices, this paper analyzes strategies for confronting wicked problems and proposes an iterative approach to the case of encryption and EA. Along the way, it illustrates the components of the debate in argument maps and demonstrate the security risks with data flow diagrams and threat analysis, focusing on one EA proposal in particular, Stefan Savage's "Lawful Device Access without Mass Surveillance Risk."

Contents

List of Tables

List of Figures

CHAPTER 1

Introduction

Certain policy issues can be described as "wicked problems." Originally coming from the field of design theory, the term "wicked problem" uses "wicked" not in the moral sense, but in the malignant, vicious, and tricky sense [1]. Unlike their "tame" counterparts which science, engineering, and traditional policymaking are well equipped to answer, wicked problems lack clear formulations, causes, resolutions, and measurements. Each attempted solution has permanent and often unintended consequences, and is likely to exist in a pattern of chronic policy failure.

Exceptional access is a wicked problem [2]. In encryption policy, exceptional access (EA) is alternative means of decryption intended for law enforcement use. Characterized by a dynamic technological environment, disagreement about underlying values, and resistance to a clear solution, the debate on EA will not go away. This thesis does not attempt to end the debate, but to structure and analyze it.

1.1 Motivation

The conflict at the heart of the encryption and EA debate is this: the same cryptographic and design principles that underlie nearly all digital security also enable an unprecedented degree of individual privacy. Encryption is a foundational tool to the integrity and confidentiality of all connected computing systems. Its increasing ubiquity in communications and storage provides clear benefits. In a world where information security is frightfully poor yet increasingly important, the necessity of strong encryption cannot be understated. However, the privacy afforded by certain encryption technologies hampers law enforcement investigations and hides wrongdoing [3] [4]. In a society that cares about bringing wrongdoers to justice, this risk should not be ignored.

The conversation regarding encryption has reached a stalemate. Governments and law enforcement agencies frequently cite the need to access encrypted data to perform their duties [5] [6] [7]. Human rights groups and technical leaders counter that a weakened encryption environ-

ment would fatally compromise privacy and security as we know it [8] [9] [10]. As the debate continues, many on both sides have become entrenched in their positions and have engaged in disingenuous attacks against their opponents.

In the long term, increased regulation of the tech industry is inevitable and regulation of encryption is possible. Despite the benefits of strong encryption, regulatory interest in the subject has not subdued. The form that regulation will take in the field of encryption depends on the good faith efforts made to equitably balance the benefits and risks involved in deploying a cryptographic system. If the technical community acts, it can lead and shape legislation rather than be subjected to it.

Most importantly, in the pursuit of data privacy, regulatory action is part of the threat model. If the technical community fails to act but regulators move forward, everyone may become subject to technically misguided, harmful laws. Bad policy is just as much a threat as weak passwords. Due to this threat, as long as lawmakers continue pursuing EA regulation, it is the responsibility of the technical community to engage in discussion and respond to the presented arguments.

For these reasons, it is important that the technical community keeps moving the debate forward.

1.2 Premises

This paper accepts and builds on the following premises. These premises are not principles for potential EA designs, but the foundation for discussing the EA debate.

1) **Cybersecurity is critical.** Due to modern culture's reliance on computer information systems, cybersecurity is critical to the wellbeing of society. Two important elements of cybersecurity are cryptography and system architecture. Policy that supports security does not undercut cryptographic integrity or require high-risk architectures.
2) **Absolute privacy is not an absolute right.** Certain rights supersede the legitimate claims of government, but privacy in all contexts does not. While individuals under a limited gov-

ernment are entitled to an expectation of privacy, an absolute right to privacy does not apply in all circumstances. Investigators should have access to some classes of data. In particular, access to certain classes of digital data is important today and will become increasingly important in the future.

3) **EA is an inherently complex problem.** The factors that make EA a wicked problem require proposed solutions to be analyzed at many levels. These factors include EA's relation to mass surveillance, potential for abuse, international consequences, economic impact, and need for transparency.
4) **Perfection is not the standard.** Wicked policy problems do not have perfect solutions; they do not even have verifiably optimal solutions. Therefore, we cannot use perfection as the standard. To quote a famous security axiom, insecurity cannot be destroyed, it can only be moved around [11]. The EA problem, like all security problems, involves finding the right balance of risk given the threats under consideration—including the threat of regulatory action.

1.3 Contribution

This thesis aims to clarify the arguments of the debate and the nature of the technical problem. After reproducing a brief U.S.–focused history of encryption regulation, technology, and conflict, I analyze strategies for tackling wicked problems and introduce argument maps and threat modeling with data flow diagrams. In the following chapters, I map the exceptional access arguments in detail and demonstrate the security risks with data flow diagrams and threat analysis, focusing on one EA proposal in particular. The thesis concludes with paths forward for research and policy that take the arguments and threats discussed into consideration.

CHAPTER 2

Background

The problem of strong encryption and exceptional access exists in a technical, historical, and regulatory context. This chapter introduces cryptography, summarizes the history of encryption and the "crypto wars," lists prominent technical EA proposals, and overviews relevant laws and regulations.

2.1 Cryptography Basics

Cryptography is the study of techniques used to communicate securely in the presence of third parties. This is performed by using a cipher to translate between plaintext and ciphertext. A cipher is a tool or algorithm that performs the translation, plaintext is the original data, and ciphertext is the encoded data. Encryption and decryption are the processes for translating from plaintext to ciphertext and back. A well-designed cipher ensures that only those parties with the correct key, or secret information, can perform encryption or decryption on the text.

There are two major cryptographic protocol families, symmetric and asymmetric. Symmetric protocols have been around for thousands of years, but asymmetric protocols were only invented in recent decades. In symmetric cryptography, encryption and decryption are performed with the same key, and both parties must have this key in order to communicate securely. In asymmetric cryptography, also known as public key cryptography, encryption and decryption are performed with two paired keys, called the public key and the private key. The public key is not secret, but due to its relationship with the private key, it can be used to establish identity and initiate encrypted communications. Using this technique, two parties can communicate privately without requiring previously agreed-upon secret information.

There are also two major cryptographic applications, securing data in motion (DIM) and data at rest (DAR). Each application presents different challenges that require different solutions. DIM typically uses long-lived asymmetric cryptography keys to perform authentication and to establish short-lived symmetric cryptography session keys. The session keys perform the ac-

tual encryption of the data in motion. Forward secrecy and replay protection are two important properties of DIM encryption protocols. Forward secrecy ensures that a leaked private key or session key does not compromise any other private key or session key; replay protection ensures that messages cannot be replayed by an attacker without detection [12]. End to end encryption (E2EE) for instant messaging services is an example of encryption for DIM.

DAR by nature must use long-lived keys for encryption. Instead of being negotiated and randomly generated at encryption-time, as DIM session keys are, these keys are either derived from user-entered passwords or are stored somewhere in computer memory. Secure storage often takes place with the assistance of dedicated hardware. Disk encryption for laptops and mobile devices is an example of encryption for DAR.

Data secrecy is not cryptography's only use, however. Data secrecy is the purpose of encryption, but encryption is only one application of cryptography. Although encryption is cryptography's "killer app," it is just a part of cryptography's usefulness to security.

Cryptography is the technical foundation for many forms of computer and network security. Security is defined in terms of several properties: authentication, integrity, non-repudiation, confidentiality, availability, and authorization [13]. These system-level properties emerge from both the composition of the system's components (architecture) and the security of the components themselves. Likewise, the security of each component emerges from the architecture of its subcomponents and the security of the subcomponents themselves. At the bottom of this chain of analysis, the security of primitive components commonly relies on cryptography.

Table 2.1 connects each security property to its cryptographic basis. While lacking direct cryptographic foundations, the property of availability indirectly relies on the other properties, and authorization schemes are typically rooted in authentication.

Violations of cryptographic integrity in primitive components, introduced by design or by accident, could have catastrophic effects. Compromised digital certificates, hashes, or encryption would enable spoofing, tampering, and information disclosure attacks. The attacks could be done for their own sake or as steps in larger attack chains. The importance of neutralizing these attacks

TABLE 2.1 The Cryptographic Basis of Security Properties

Property	Cryptographic Basis
Authentication	Digital certificates
Integrity	Cryptographic hashes
Non-repudiation	Digital signatures
Confidentiality	Encryption
Availability	*based on architecture*
Authorization	*rooted in authentication*

is clear when they result in interference with elections [14], multi-billion dollar disruptions of business [15], and hospital network ransoms that disrupt care of patients [16].

Cryptography has an absolute, mathematical power—a power that is necessary in the realm of security, but objectionable in the realm of privacy. Encryption's dual role as an enabler of privacy and cornerstone of security is at the heart of the EA debate.

2.2 Encryption History

The section provides a brief history of encryption from ancient to modern times.

2.2.1 Encryption In the Past

Computerized encryption is a new technology, but the field of cryptography is old, since demand for privacy is as old as communication itself. The most well-known ancient example of rudimentary encryption is the Caesar cipher, named after the character substitution technique Julius Caesar used to protect private correspondence [17]. Significant developments include the first formal cryptographic study by Arab scholars in the eighth century, advancements made out of necessity during the twentieth century's world wars, and the application of computers to cryptographic problems [18]. Claude Shannon formalized the modern "mathematical analysis of cryptography" in 1949 [19] and Whitfield Diffie and Martin Hellman published research on public key cryptography in 1976 [20]. The discovery of public key cryptography was an important advance. Combined with computer networking and personal computing advances in the 1980s,

it put the power of strong encryption not just in the hands of governments and militaries, but of ordinary people.

However, this power enables very strong individual privacy. Government is inherently uncomfortable with individual privacy; therefore, the use of encryption for private purposes has a contentious history. In 1587, Mary Queen of Scots was convicted of treason based on evidence from decrypted letters, and in 1807, the prosecutors who tried Aaron Burr for treason attempted to force testimony from his secretary on the contents of encrypted messages [21].

2.2.2 The First Crypto War

These circumstances—government discomfort with absolute privacy, rapidly increasing availability of strong encryption, and a blossoming computer industry foundationally reliant on cryptography—came to a head in what has become known as the first "crypto war."

In 1976, Diffie and Hellmann published their seminal research in public key cryptography. That same year, the U.S. Congress passed the Arms Export Control Act (AECA) and declared that strong cryptography is subject to export controls [22]. The first crypto war began in 1991, when the U.S. Senate introduced, but did not pass, a bill mandating access to plain text contents when authorized by law. In response, Philip Zimmermann released Pretty Good Privacy (PGP), e-mail encryption software, in order that strong cryptography be "made available to the American public before it became illegal to use" [23]. In 1993, the Clinton administration introduced the Clipper Chip [24] with the goal of "providing the public with strong cryptographic tools without sacrificing the ability of law enforcement and intelligence agencies to access unencrypted versions of those communications" [25]. Citing the foundational role of cryptography in security—and the potential of human rights abuses resulting from compromised privacy—industrial and technical leaders reacted negatively to the initiative [22] [23]. When a prominent security researcher discovered flaws that allowed users to subvert the Clipper Chip mechanisms [26], the proposal died.

Despite the failure of the Clipper Chip, the debate over export controls and access to strong

encryption continued, primarily focused on various key escrow proposals [25]. In 1996, two pro-encryption bills were introduced in the U.S. Congress, one in the Senate and one in the House. The Senate saw S.1726, the Promotion of Commerce On-Line in the Digital Era Act (Pro-C0DE Act) of 1996, which sought to abolish the export controls on encryption software [27]. The House saw HR.3011, the Security and Freedom Through Encryption Act (SAFE Act) of 1996, which similarly sought to remove export controls, but further sought to explicitly allow arbitrarily strong encryption for all legal activity and to preclude mandatory EA schemes such as the Clipper Chip [28]. Zimmermann, the author of PGP, who had by this time endured an investigation by the Customs Service for publishing his work, testified before the Senate in favor of the Pro-C0DE Act [23]. In November of 1996, the Clinton administration released an executive order effectively removing export controls on encryption products along the lines of the Pro-C0DE Act, which never came to pass [29].

From 1996 to 1999, the SAFE Act was proposed several times, was discussed at hearings, and gained support [22]. By this time, there was "an overwhelming amount of evidence against moving ahead with any key escrow schemes" [25], and in 1999 the Clinton administration changed course again, adopting almost all SAFE Act proposals [22]. This development marked the end of the first crypto war.

2.2.3 The Second Crypto War

Two developments paved the way for the second crypto war. The first was the result of inaction: when the Clinton administration changed its encryption policy, the U.S. House dropped the SAFE Act [28]. The Pro-C0DE Act and other encryption-related bills went unpassed as well, as elaborated in Section 2.4.2. This legislative failure meant that encryption policy was written not in the pen of law, but in the pencil of executive order.

The second development was the terror attacks of September 11, 2001. The events of that day occurred in the context of expanding law enforcement powers fueled for decades by all three branches of government. Presidents promoted the idea of being "tough on crime" and launched

a war on drugs; legislators passed bills such as 1978's Foreign Intelligence Surveillance Act (FISA), which provided broad surveillance powers over foreign nationals, and in some cases U.S. citizens [30]; and the judiciary practiced a "jurisprudence of crime control" that gave police broad leeway [31].

In this context of expanded surveillance, the scale of the September 11 attacks seemed to justify yet greater investigatory powers [32]. October of 2001 saw passage of the USA PATRIOT Act, which had several significant impacts: (1) it weakened the limitation for using FISA requests on U.S. citizens; (2) it expanded the scope of what could be compelled via FISA orders; (3) it authorized "roving" wiretaps; and (4) it increased the power of National Security Letters (NSLs), which can be used without judicial review to compel information from digital service providers while precluding any public disclosure of the event [33] [34]. The government was performing more surveillance than ever, and even these weakened limitations would be repeatedly violated [34] [35].

The weakness of data protection laws and absence of encryption protection laws left the door open for a second crypto war. Increased government surveillance set events in motion toward conflict. These two developments prepared the way, but it was the 2013 Snowden revelations that constituted the crossing of the threshold. Though policies such as the U.S. National Security Agency (NSA)'s warrantless wiretapping caused a stir, it was the mass data collection under the agency's PRISM and related programs that caused the real public outcry [36]. With the public interest focused on digital privacy, encryption promised to be a technical solution. U.S. tech companies responded by introducing default device encryption for data at rest and end to end encryption for data in motion.

The emergence of strong encryption caused the first crypto war; its proliferation is causing the second.

The U.S. corporate response to Snowden should not be overly construed as a morally motivated defense of civil rights. Their behavior is a matter of several practical factors, including market pressure, cultural pressure, and the advancement in available encryption technology [37].

Another factor is the pursuit of basic digital security. Recall encryption and cryptography's critical role in security as described in Section 2.1. When lawmakers question technical leaders about their companies' encryption policies, executives have repeatedly appealed to the fact that strong cryptography is a necessity for security [38].

2.2.4 Current Context

Several events and arguments have come to characterize the second crypto war.

"Security vs. Security". The relationship between security and privacy is sometimes viewed as antagonistic, an assumption implicit in the "nothing-to-hide" argument. However, discussions in recent years have shown that the debate is more about "Security vs. Security" than "Security vs. Privacy" [39]. In this context, there are two types of security. First, public security (often referred to as "safety" in this paper), which is the pursuit of law enforcement. Second, cybersecurity, which the pursuit of the technical community. Both sides of the debate have by now acknowledged that privacy and public security are not always in conflict. In fact, it is the relationship between public security and cybersecurity—which in return affects public security—that be more important [40].

Apple vs. FBI. The 2015 San Bernardino terror attack resulted in the first major battle of the second crypto war. The attacker was killed, leaving behind a locked iPhone. The Federal Bureau of Investigation (FBI) issued an order under the All Writs Act to compel Apple to unlock the device, which was among the first generation of Apple's fully encrypted iPhones. Apple objected on grounds that it was "unreasonably burdensome" and would undercut the integrity of all iOS devices [38]. The case occupied U.S. District courts, the media, and the attention of the political world from February 16, 2016, when the warrant was issued, to March 28, when the FBI announced they had gained access to the phone through alternate means [41]. Although the phone proved not to contain any important data [38], the high profile case featured two characteristic elements of the new crypto wars—terrorism and device encryption. Shortly after the case ended, a pair of Republican and Democratic senators jointly released a discussion draft of a bill

that would have forced Apple to comply [42]. The draft did not make it to the Senate floor, and the unresolved nature of the court case left the legal debate unresolved.

The Four Horsemen. In the 1990s, an influential encryption advocate coined the phrase "the Four Horsemen of the Infocalypse" to describe four reasons that governments and law enforcement agencies use to undercut public support for strong encryption [43]. The original list includes terrorists, pedophiles, drug dealers, and money launderers, though many substitute kidnappers for money launderers [44]. Reflecting the times, the first crypto war emphasized drug trafficking whereas the second crypto war emphasizes terrorism and child pornography (increasingly referred to as child sexual abuse material (CSAM)) [38]. The focus on terrorism is likely a result of the September 11 terror attacks as well as the San Bernardino terror attack that launched the Apple vs. FBI case. The focus on CSAM is likely a result of the growth of the "dark web" and a revelatory 2019 investigation by the *New York Times* [4].

DIM vs. DAR. As noted in Section 2.1, securing data in motion and data at rest are two different challenges that require different solutions. Therefore, both technical and policy proposals often split their recommendations along these lines [45] [46]. Discussion of EA for DIM typically involves E2EE, whereas for DAR it typically involves disk encryption of mobile phones. The focus of law enforcement in the U.S. has pendulated between these several times [40]. A research group at Carnegie Mellon with participants from both sides of the debate has identified EA for DAR as the more tractable problem [45].

Volatile Politics. Finally, the second crypto war is taking place amidst a political landscape marked by uncertainty, extremism, misinformation, and a pandemic that will have unknown long-term impacts. Since government is part of the broader data security threat model, its behavior is important. Unfortunately, it is difficult for the technical community to engage productively with policymakers due to present political dynamics and the lack of reliable data demonstrating the extent of law enforcement's difficulties [47].

That brings us to where the debate stands today. A December 2019 U.S. Senate Judiciary Committee featured the top two U.S. parties both expressing anger over whether data should be

"beyond the reach of the law." Senators threatened tech executives with statements such as "get your act together, or we will gladly get your act together for you" [48]. In March 2020, the Republican atop the Senate Judiciary Committee introduced S.3398, the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act) of 2020, which seeks to establish a 16-chair committee with the power to revoke online platforms' liability protection for user-submitted content if the committee determines the platform is not doing enough to fight CSAM [49]. As illustrated by the previously mentioned *New York Times* feature [4] that likely triggered the December 2019 hearing, the problem is enormous. However, critics largely saw the EARN IT Act as an attempt to indirectly yet effectively outlaw E2EE [50] [51]. In response, legislators narrowed the focus of the EARN IT Act, but only after unveiling the Lawful Access to Encrypted Data Act (LAED Act)—a direct attack on strong encryption calling for broad exceptional access capabilities.

2.3 Approaches to Exceptional Access

There are several technical approaches to EA. This section organizes approaches into three categories—key escrow, cryptographic recovery without a key, or non-cryptographic means of acquiring plaintext.

2.3.1 Types of Key Escrow

Key escrow is the most obvious way to implement EA. It involves storing additional copies of the encryption keys. Alternatively, rather than directly storing copies, key escrow may involve storing information that can be used to derive additional copies. Key escrow can be subdivided into various types according to where the escrowed information is stored.

- **Trusted-party key escrow**

  Any scheme that relies on the fidelity and security of information held by an entity besides the data owner (in the case of DAR) or sender or receiver (in the case of DIM) is a "trusted-party" key escrow approach. Though there is a wide variety of implementation options within this category [52]—secret or open protocol, hardware-enabled or software-only, single- key or split-key, government or third-party escrow—the foundation of the effectiveness of these approaches lies in the security of the trusted party. The Clipper Chip is one example, being a secret-protocol hardware-enabled split-key government escrow system [52].

- **Distributed key escrow**

  Some schemes compensate for the risk of concentrated sensitive information by massively distributing the secret information. In this arrangement, trust is put in the distributed system, not in any single party. Such systems offer high data availability while making covert key recovery difficult. This approach was introduced in the first crypto war [53] and has modern blockchain [54] and distributed device [55] variations. These approaches are not as thoroughly explored as trusted-party key escrow.

- **Device key escrow**

  The third type of key escrow is device-based. In device key escrow, key information is held not by trusted parties or distributed systems, but on the device itself in specialized hardware. Advances in secure hardware "enclaves" since the first crypto war have enabled secure local key storage. Approaches relying on hardware primarily target DAR and may include time elements and split keys with trusted parties as well [56] [57].

2.3.2 Non-Escrow Cryptographic Data Recovery

Though key escrow is the most discussed EA approach, alternative technical means have been proposed.

- **Translucent cryptography**

  Research in the first crypto war included the introduction of "translucent" cryptography, in which an observer could surveil some but not all communications using statistical cryptographic methods [58]. Under this scheme, no keys are escrowed, but law enforcement could recover a predetermined percentage of plaintext data. That percentage would be designed to balance privacy, security, and safety. This research, though more experimental than key escrow proposals, was explicitly pursued to demonstrate that alternatives to key escrow do exist [58].

- **Cryptographic "crumple zones"**

  A recent proposal adopts the idea of crumple zones from automotive engineering—"in an emergency situation the construction should break a little bit in order to protect the integrity of the system as a whole and the safety of its human users" [59]. Similar to the translucent approach, no keys are escrowed and only passive surveillance is possible. Keys are generated in a manner that makes messages inherently recoverable, but only after extreme up front costs and significant marginal costs.

2.3.3 Alternative Approaches

The following approaches do not use EA at all, but are alternative technical or legal mechanisms that can be used towards the same goal.

- **Lawful hacking**

  Lawful hacking is one way to access plaintext without EA. Under lawful hacking, instead of having access to plaintext data via an alternative means of decryption, law enforcement is allowed to perform otherwise-illegal hacking activity in order to find the key, compromise a device, or intercept plaintext versions of the data [21]. While some see this as a viable middle ground [60], encouraging law enforcement to exploit vulnerabilities can create misaligned incentives. If law enforcement opposes strong security in general, it could foster the exploit market while costing ordinary users money and security [61].

- **Compelled password disclosure**

  In some cases, a suspect in custody may have the ability to access the desired encrypted information via a key, personal identification number (PIN), or password. In these cases, authorities sometimes compel the suspect to disclose the password. In the U.S., this approach draws debates about the Fifth Amendment right against self-incrimination [62] [63]. Of course, this approach cannot address DIM or situations in which the knowledgeable party is not in custody.

- **Alternative paths to plaintext**

  Simpler methods than computer hacking or legal coercion can be used: encrypted data may exist in plaintext copies elsewhere, or authorities may seize equipment while it is unlocked [21]. This approach relies on law enforcement's skills in investigation and sting operations. This approach is used successfully today. In 2017, an international law enforcement operation used this technique to take down a large illicit online drug market [64]. This approach also does not address DIM and requires well-executed operations.

2.4 Regulatory Environment

The following sections list laws which directly or indirectly affect the use of encryption. Though this thesis is U.S.–focused, it is worth briefly touching on the regulatory environment of other countries. EA is an international problem, as digital technology has little respect for political borders. Sections 2.4.1-2.4.3 describe the regulatory environment in the U.S. and Section 2.4.4 describes regulations around the world.

2.4.1 Enacted U.S. Regulations

The following laws and regulations have been applied to cases involving surveillance, cryptography, and access to encrypted information:

- 1789: **All Writs Act (AWA)** [65]

  The AWA is a short law designed to grant federal courts the right to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law," creating a legal framework for providing data to law enforcement. The AWA was famously cited in the Apple vs. FBI case, though its applicability to EA in general is unsettled [66].

- 1791: **Bill of Rights: Amendments I, IV, and V** [67]

  Three Bill of Rights amendments are frequently cited in the EA debate. I: freedom of speech; IV: protection from unreasonable searches and seizures and requirements for warrants; and V: the right against self-incrimination.

- 1976: **Arms Export Control Act (AECA)** [68]

  The AECA expanded arms export controls and created the International Traffic in Arms Regulations (ITAR) regulations framework. Encryption products were classified as arms and subjected to export controls [22].

- 1978: **Foreign Intelligence Surveillance Act (FISA)** [30]

  This statute allows the executive branch "to authorize electronic surveillance for foreign intelligence purposes without a court order, in some circumstances." FISA applications take place in secret, and may be conducted against U.S. citizens if foreign intelligence is the "primary purpose" [34]. FISA has been the subject of frequent FBI abuse [34] [35].

- 1986: **Electronic Communications Privacy Act (ECPA)** [69]

  ECPA includes the Stored Communications Act and Pen Register Act, and amends the switchboard-era Wiretap Act. ECPA provides explicit protections for private electronic communications data, and updated definitions to contemporary technology. It grants law enforcement explicit access to certain data as well; some terminology has aged poorly with technological evolution, making the access increasingly permissive [34].

- 1994: **Communications Assistance for Law Enforcement Act (CALEA)** [70]

  CALEA mandates that telecommunications carriers enable the government to "intercept all of the subscriber's wire and electronic communications" in a manner that "protects the privacy and security" of communications not authorized to be intercepted. The law does not authorize law enforcement to compel use of any specific technologies, which meant that the Clipper Chip proposal issued a year earlier could not be made mandatory through CALEA. CALEA specifically excludes "information services" from its interception requirement which has included internet platforms, though that exclusion is currently under attack [71].

- 2001: **Uniting and Strengthening America by Providing Appropriate Tools Required**

to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) [33]

Written in the aftermath of September 11, the USA PATRIOT Act broadly expanded U.S. government surveillance powers in the 25 sections of "Title II: Enhanced Surveillance Procedures." The act notably expanded FISA order scope (Section 206), duration (207), and use on U.S. citizens (218). Section 215 enables court orders requiring business records, but the Snowden leaks revealed that the government had been secretly using a non-standard definition of "business records" in order "to justify requests for domestic telephone metadata delivered in bulk, not individualized requests" [36].

- 2008: **FISA Amendments Act (FISAAA)** [72]

  Like the USA PATRIOT Act before it, FISAAA expanded FISA powers once again. It additionally provided "telephone companies retroactive immunity for participating in the warrantless surveillance" on any international communication, a policy established in 2001 under another loose, secret interpretation of FISA, "as well as creating prospective immunity for FISAAA activities" [36].

- 2015: **Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act (USA FREEDOM Act)** [73]

  The USA FREEDOM Act, introduced by the same U.S. House representative as the USA PATRIOT Act, passed the Senate almost two years to the day after Snowden's leaks began. It contains many reforms to FISA and the use of NSLs. Most notably, it ends the interpretation of section 215 of the USA PATRIOT Act that enabled mass collection of telephone metadata.

2.4.2 Unsuccessful U.S. Regulation Attempts

The following are proposed laws and regulations that did not go into effect or are still in process:

- 1993: **The Clipper Chip** [24]

  As described in Section 2.2.2, the Clipper Chip was a voluntary EA initiative from the White House. The initiative targeted DIM and established the Escrowed Encryption Standard, which includes an encrypted copy of the session key in the message [26]. The initiative prompted debate but received a largely hostile reception [22]. When a security researcher discovered flaws that allowed users to subvert the Clipper Chip mechanisms, the proposal died [26].

- 1996: **The Security and Freedom Through Encryption Act (SAFE Act)** [28]

  The SAFE Act would have broadly protected "use any encryption regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used," excepting "the unlawful use of encryption in furtherance of a criminal act." It also would have lifted export controls. The bill grew support as it was reintroduced in consecutive congresses, but was abandoned when the Clinton administration adopted the act's pro-encryption policies in 1999 [22].

- 1996: **The Promotion of Commerce On-Line in the Digital Era Act (Pro-C0DE Act)** [27]

  The Senate's Pro-C0DE Act was very similar to House's SAFE Act, though it focused primarily on removing export controls, and used slightly weaker language protecting all forms of encryption. Like the SAFE Act, it was abandoned when the Clinton administration adopted the act's export control policies in 1996 [25].

- 1999: **Cyberspace Electronic Security Act (CESA)** [74]

  CESA was a legislative proposal by the Clinton administration introduced alongside the executive order that led to the abandonment of the SAFE Act. Section 102 lays out the government position precisely: encryption is an important tool for information security, but is also used to "hide unlawful activity by terrorists, drug traffickers, child pornographers, and other criminals" (the Four Horsemen), and therefore "appropriate means must be available to fulfill these law enforcement objectives." The bill would establish a voluntary-participation third-party key escrow system with "recovery agents" that would provide law enforcement with access to plaintext. Access would be compelled through a variety of mechanisms, including warrantless mechanisms through FISA. The White House failed to attract a member of Congress to officially sponsor the bill.

- 2000: **Enhancement of Privacy and Public Safety in Cyberspace Act** [75]

  After CESA failed, the White House proposed watered-down legislation that was successfully sponsored by a senator. This bill would have amended the Electronic Communications Privacy Act (ECPA) and Computer Fraud and Abuse Act (CFAA). It would have made relatively modest changes to government data access requirements. Though it received congressional sponsorship, even the sponsor was critical of parts of the bill, and it died in committee [76].

- 2016: **Compliance with Court Orders Act (discussion draft)** [42]

  Though this bill was not officially proposed, it represents one of the first legislative attempts to regulate encryption in the second crypto war. This draft was released shortly after the close of the Apple vs. FBI case, and would have compelled Apple to unlock the suspect's phone. Though it would not mandate a specific technical approach, the bill would have mandated that manufacturers and service providers be able to provide EA. This mandate notably goes beyond several regulatory proposals in the first crypto war by forcing platform and application developers to comply. Previewing a common phrase in recent EA arguments [48], the draft's authors both used the phrase "above the law" in promotion of the bill.

- 2018: **The Secure Data Act** [77]

  Proposed in reaction to the Compliance with Court Orders Act and anti-encryption sentiment, this bill would have provided protections against "mandating the deployment of vulnerabilities in data security technologies" at the federal level. It stopped short of explicitly protecting all forms of encryption.

- 2019: **The Ensuring National Constitutional Rights for Your Private Telecommunications Act (ENCRYPT Act)** [78]

  This bill is designed to "preempt State data security vulnerability mandates and decryption requirements," being a state-level version of the Secure Data Act. This bill goes further to explicitly disallow EA requirements in state law.

- 2020: **The Lawful Access to Encrypted Data Act (LAED Act)** [79]

  The LAED Act is a direct attack on encryption and the spiritual successor of the Compliance with Court Orders Act. It was introduced by the chair of the Senate Judiciary Committee, also sponsor of the EARN IT Act and one of the outspoken encryption critics during the 2019 Senate hearing on encryption and EA. The LAED Act specifically addresses DAR and DIM by forcing device, operating system, and application developers to implement the ability to decrypt all data stored or passing through the device or software system "concurrently with their transmission" "unless the independent actions of an unaffiliated entity make it technically impossible to do so." The act neither mandates nor recommends any technical approach to providing this capability.

2.4.3 The U.S. Judicial Environment

The above history and section on U.S. law encompasses the executive and legislative branches' influence on surveillance and cryptography. However, a complete portrait of government encryption policy must include the influence of the judiciary branch. The judiciary branch influences policy through interpretation of laws and creation of legal doctrine. This section describes this influence, reviews how it has affected cryptography policy, and analyzes where cryptographic jurisprudence may go from here.

The primary judiciary function is to adjudicate the law through the determination of facts and interpretation of authoritative legal texts. However, whether it is contested or conceded, condemned or condoned, the judicial branch also establishes legal doctrine and actively enforces rulings in a manner that amounts to creation of public policy [80]. Due to Congress's clear authority over telecommunications and federal investigatory powers, the courts are most likely to exert influence in this area through interpretation of current law. This interpretation will both determine how present law is enforced and draw constitutional boundaries around any actions the executive or legislative branches undertake.

Judicial influence on encryption policy is primarily mediated through the Fourth Amendment,

particularly regarding the interpretation of a person's "effects," what is "reasonable," and what defines a "search." The Supreme Court's interpretation and implementation of the Amendment has changed over time. Legal scholars Craig Curtis and Michael Gizzi conducted an in-depth analysis of the Court's jurisprudence from the 1960s Warren Court, through the influential 1980s Rehnquist Court, to the mid-2010s Roberts Court [31]. Their analysis revealed a deep proclivity towards crime control that is only recently thawing. This gradual return to decisions favoring civil liberties, caused by evolution of technology, of the court, and of the justices themselves, has been favorable for data privacy. Recent cases have increasingly sided with defendants, caused justices to strain to show that they understand technology, and increased the categories of protected digital data [31]. 2018's potentially landmark *Carpenter v. United States* may be the most impactful yet. Though the case only resulted in a narrow decision against unwarranted cell phone location data tracking, the Court's decision undermines the pre-digital era third-party doctrine, which holds that Fourth Amendment protection is forfeit when the data is willingly given to a third-party [81].

As this relates to EA, Fourth Amendment interpretation determines the threshold at which authorities require a warrant, but does not specify what demands they can or cannot make once they have one. As mentioned above, the FBI argued in the San Bernardino case that the All Writs Act (AWA) grants it authority to demand access to plaintext, though others argue that CALEA explicitly precludes this kind of demand [82]. Since the FBI dropped the case, the matter is not formally settled, though the consensus is that legislation such as the LAED Act is required before courts would uphold such a command.

The second most salient legal issue is the Fifth Amendment right against self-incrimination, which arises in cases of compelled password disclosure. This question has not yet reached the Supreme Court, and state courts have ruled compelled disclosure as constitutional in some cases [63] [83] and unconstitutional in others [84] [85].

It is to be expected that judicial influence on privacy and technology is evolving. To explain the fluctuating state of legal interpretation as it relates to EA, Vashek Matyas et al. make the

helpful distinction between legal rules and principles [66]:

> The tension between technical and legal views of sensitive issues such as encryption and surveillance is illuminated by applying the jurisprudential lens. … Liberal legal systems, manifesting what is generally understood as "the rule of law," are actually composed of both rules and principles. Legal "rules" can be understood as logical propositions that are expected to yield answers about what is and is not permitted using formal reasoning capabilities. By contrast, legal "principles" articulate values and policies that must be reflected in a legal system but do not necessarily dictate an unambiguous outcome in any given case.

Rules are the low-level implementation of principles. When the underlying facts of the situation change, as they do by definition for wicked problems, the rules become out of sync with the principles that bade them. Recent flux in judicial rulings surrounding surveillance and technology, particularly around the Fourth Amendment, prove that the courts are in the process of updating interpretations of rules in light of the new facts; which principles they will ultimately favor remains to be seen, but rulings like *Carpenter* show a willingness to protect privacy.

There are three types of cases through which the judicial branch could have a strong effect on the future of digital privacy policy. First, Fourth Amendment cases will establish classes of protected data and thresholds for warrants. Second, a Supreme Court Fifth Amendment case could settle under what circumstances, if any, a password could be compelled. Third, a surprise AWA ruling could open the door to demands for access, though legislation like LAED Act is more likely to have this effect.

2.4.4 Regulations around the World

This thesis focuses on U.S. policy, but EA technologies and policies have international impacts. The following is a brief account of the regulatory environment in various geographical jurisdictions around the world based primarily on a 2016 analysis by the Law Library of Congress

[86]. A separate 2017 study found that globally, more than half the world's internet users lived in a country where some form of plaintext recovery is mandated [87].

- **Five Eyes Countries** [86]

  In 1946 The U.S. formalized an intelligence-sharing operation with the U.K. in the BRUSA (now UKUSA) Agreement. Over the following 10 years, Australia, Canada, and New Zealand were made full partners to this agreement, which has become known as "Five Eyes" [88]. Due to the close relationship between the intelligence and law enforcement agencies of these countries, the member's encryption policies are relevant to each another.

  The U.K. government has the explicit ability to force decryption, perform lawful hacking, and mandate EA though "technical capability notices" introduced in 2016's Investigatory Powers Act [89]. Australia has weaker powers through a variety of laws, and in 2018 passed the Assistance and Access Act which created very similar "technical capability notices" [90]. Canadian law requires cooperation between telecommunications providers and law enforcement but does not directly address encryption. Canada has traditionally supported strong encryption, but the pressure of the second crypto war is straining that support [91].

- **European Countries** [86]

  Among European countries, France and Russia join the U.K. in having access mandates [87]. France, Belgium, Germany, and Sweden require cooperation between telecommunications providers and law enforcement; for France, Belgium, and Germany, that includes decrypting network traffic when possible. France, Germany, and Sweden each have some level of lawful hacking capability. There is no E.U. legislation that requires key disclosure or decryption of network traffic.

- **Asian Countries** [86]

  Japanese authorities require cooperation and can request access to decrypted data, but subjects are not punished for declining such requests. Taiwanese regulation does not specifically address encryption, but does mandate that telecommunications providers provide interfaces "with functions that can cooperate with interception." Chinese authorities have great access to plaintext data by virtue of the political structure of the state, as well as through explicit requirements in recent anti-terrorism and cybersecurity laws [87].

- **Other Countries** [86]

  Brazil, South Africa, and Israel require cooperation between telecommunications providers and law enforcement. Brazil law does not specifically address encryption, though it does require "the technological resources necessary to suspend telecommunications confidentiality in accordance with the law." South Africa mandates decryption when possible. Israeli authorities can issue warrants for access to data or use warrantless orders similar to U.S. FISA mechanisms. Israel also has well developed lawful hacking capabilities and a centralized forensics laboratory [92].

CHAPTER 3

Strategy for Tackling Wicked Problems

Before detailing the specific arguments used in the EA debate, it is worth achieving a better understanding of wicked problems in general. What are they, and why do the problems surrounding encryption, privacy, and EA fall into this category? What approaches to tackling wicked problems succeed and fail? How can we strategically confront them and make real progress? This chapter seeks to answer these questions.

3.1 Wicked Problems

Wicked problems were previously introduced as pernicious and tricky issues that resist straightforward solutions. This section analyzes the nature of wicked problems and approaches to tackling them.

3.1.1 Characteristics

Rittel's categorization of wicked problems grew out of frustration with their resistance to traditional problem solving methods. Since the Enlightenment, society has applied the scientific method to problems of every kind; the sweeping application of scientific analysis has delivered reliable clean water, improved crop yields, shaped government structures, and bestowed material wealth previously unimaginable. With these material problems largely solved in the twentieth century, believers in the power of reason thought this progress would continue in the realm of public planning. Policymaking would function by setting goals, identifying problems, evaluating alternatives, implementing solutions, and analyzing outcomes in order to correct errors. Functioning as a continuous process, this approach was primed to revolutionize governing the same way it did industry, agriculture, and economics—until it didn't. In the context of what he describes as an "anti-professional movement," Rittel explains how the scientific method has failed:

> A great many barriers keep us from perfecting such a planning/governing system: theory is inadequate for decent forecasting; our intelligence is insufficient to our

> tasks; plurality of objectives held by pluralities of politics makes it impossible to pursue unitary aims; and so on. The difficulties attached to rationality are tenacious, and we have so far been unable to get untangled from their web. This is partly because the classical paradigm of science and engineering—the paradigm that has underlain modern professionalism—is not applicable to the problems of open societal systems. One reason the publics have been attacking the social professions, we believe, is that the cognitive and occupational styles of the professions—mimicking the cognitive style of science and the occupational style of engineering—have just not worked on a wide array of social problems. The lay customers are complaining because planners and other professionals have not succeeded in solving the problems they claimed they could solve. We shall want to suggest that the social professions were misled somewhere along the line into assuming they could be applied scientists—that they could solve problems in the ways scientists can solve their sorts of problems. The error has been a serious one. [1]

When applied to social problems, the prescribed method—here defined as setting goals, identifying problems, evaluating alternatives, implementing solutions, and analyzing outcomes—fails at every step. In the U.S., a nation composed of many varying cultures and subcultures and politically dominated by two mutually hostile parties, agreeing on goals is a challenge in itself. When goals are set, we often discover that we are contending with wicked problems that defy the process at each remaining step. Rittel provides a list of ten characteristics of problems in this category [1]:

1) There is no definitive formulation of a wicked problem [and each formulation presupposes a solution].
2) Wicked problems have no stopping rule.
3) Solutions to wicked problems are not true-or-false, but good-or-bad.
4) There is no immediate and no ultimate test of a solution to a wicked problem.

5) Every solution to a wicked problem is a "one-shot operation"; because there is no opportunity to learn by trial-and-error, every attempt counts significantly.
6) Wicked problems do not have an enumerable (or an exhaustively describable) set of potential solutions, nor is there a well-described set of permissible operations that may be incorporated into the plan.
7) Every wicked problem is essentially unique.
8) Every wicked problem can be considered to be a symptom of another problem.
9) The existence of a discrepancy representing a wicked problem can be explained in numerous ways. The choice of explanation determines the nature of the problem's resolution.
10) The [decision maker] has no right to be wrong [i.e., they are liable for the consequences of their decisions].

In summary, (1) the wicked problems are impossible to definitively identify, (2) potential solutions are impossible to definitively evaluate, (3) every action or inaction has permanent effects, and (4) solutions are importable from one problem to another. The policy version of the scientific method cannot be used under these conditions. The "wicked" problem's counterpart is the "tame" problem. "Tame" does not imply easy; it only means that the scientific approach will be effective.

Several of wicked problems' characteristics are results of the fact that we have no accurate predictive model of the world and human behavior. This is self-evident. The more important insight is one step removed: precisely because there is an inexhaustible set of potential solutions, the problem definition—that is, the set of information required to produce a solution—is not self-contained. Each proposed solution demands that new research and context be fed back into the problem definition. This feedback from proposal to definition violates the linearity of the traditional approach. One cannot reason from problem statement to proposals to a solution; instead, one is forced to constantly refine the problem statement based on the content of proposals themselves.

A 2018 study by the Australian government uses climate change as an example of a wicked problem [93]. Say the problem is initially formulated as long-term change to the environment caused by the effects of accumulating greenhouse gasses. Responses typically take one of three broad forms [93]. First, profligate behavior in consumeristic societies must be reigned in at a local and personal level. Second, global inter-governmental coordination is the only solution, as individual changes will have no impact. Third, the situation is overblown by idealists and power-mongers, and technological progress and adaptive markets will handle any negative effects that come to pass. Which response is correct? It is impossible to tell by evaluating the problem statement. How much do individual choices contribute to greenhouse gas emissions? How effective are international accords? How costly will the changes be, and how capable is technology to respond? Evaluating the validity of each proposal requires updates to the problem statement itself.

Wicked problems always consist of subproblems, which may be tame or wicked themselves. For example, climate change has many subproblems. Developing clean energy technology is a tame subproblem; implementing any solution in a way that doesn't leave vast swaths of people behind is a wicked subproblem. Wicked problems quickly grow in complexity with the number of subproblems that comprise them. Truly imposing wicked problems are composed of a tangle of contributing factors, and despite the presence of tame elements, they pose a large number of difficult challenges.

3.1.2 Encryption and EA as a Wicked Problem

Dogged by concerns over privacy, security, safety, and trust, encryption and the presupposed solution of EA is a wicked problem. It has each of the characteristics from Rittel's list above:

1) There is no formulation that encapsulates the problem of encryption's interplay with privacy, security, safety, and trust.
2) Balancing each value in the face of constantly evolving technology is a never-ending cycle.
3) EA or other proposals cannot definitively solve the problem.
4) EA or other proposals cannot be objectively tested.

5) Every policy implementation has irreversible effects.
6) There is an inexhaustible set of potential solutions to the problem.
7) Solutions from other domains do not apply directly to this problem.
8) The need for EA or some alternative is a symptom of differing values, rapid technological change, and criminal behavior.
9) The problem can be framed many ways: as insufficient investigatory access to digital data (presupposing EA as the solution), outdated cyberlaw (presupposing legal hacking or compelled password disclosure as solutions), and more.
10) The decisions of regulators and technologists have real impacts in the world today.

Cybersecurity law scholar Alan Rozenshtein argues at length for treating encryption and EA as a wicked problem [2]. He divides the root issues into three categories. First, there is disagreement on what the goals should be (and even basic premises). Sides do not agree on how much to value competing notions of security. Regarding the basic facts, sides do not agree on whether encryption is hiding so much evidence that law enforcement is "going dark," as one side puts it, or whether technological change overall has created a "golden age for surveillance," as their opponents argue. Second, information is "uncertain and diffuse." Comprehensive data regarding encryption's effect on investigations is unavailable. Although the consensus is that we are not presently capable of acceptably secure EA, that consensus could change, especially considering that EA as a field is under-researched. Third, the problem cannot be definitively solved. Evolving values and technology mean that this policy area is always up for renegotiation.

Encryption technology is particularly sensitive to the irreversible effects of policy implementation. Technology deployments have long tails and attackers have the ability to record and store data for later analysis. In one investigation, Australian police cracked a cold case based on evidence acquired from a mobile device that they cracked five years after it was seized [94]. In this case, it was lawful authorities that benefitted from a vulnerability. However, if miscalculated EA mandates result in vulnerabilities such as this, attackers will benefit, not just law enforcement.

Rozenshtein reflects on the wicked problem diagnosis optimistically:

> Recognizing that something is a wicked problem is not an admission of its insolubility; rather, it's just a realistic appreciation of its challenges. Progress on difficult social problems reflects, almost by definition, progress on wicked problems, whether economic inequality, environmental degradation, or government access to data. Progress can be made, but it first requires a clear-eyed appreciation of the nature of the problem and the nature of its challenges. [2]

Reality must be accepted before it can be dealt with. [95]. We have by now embraced the reality of wicked problems. The next two sections investigate strategies for dealing with this reality.

3.2 Failure of Current Policymaking Approaches

This section describes two common policymaking approaches, the classical analytic method and incrementalism.

3.2.1 The Classical Analytic Method

The classical analytic method [80] (also known as "the modern-classical model of planning" [1], "the rational-comprehensive method" [96], "traditional policy analysis" [2], or "linear thinking" [93]) has already been introduced. It is the reason-based method that functions by setting goals, identifying problems, evaluating alternatives, implementing solutions, and analyzing outcomes in order to correct errors. Figure 3.1 illustrates this approach in the context of encryption and EA. It has a purely linear flow from problem to solution except for the "refinement" step, in which the method analyzes outcomes and corrects errors. However, it is important to note that refinement represents a reinforcement, as opposed to a reassessment, of the chosen solution.

The shortcomings of the classical analytic method were discussed in Section 3.1.1. It fails due to disagreement over goals, the dependence of the problem definition on the potential solutions generated (violating the linear flow), the inability to evaluate alternatives, and the lack of a definitive stopping rule.

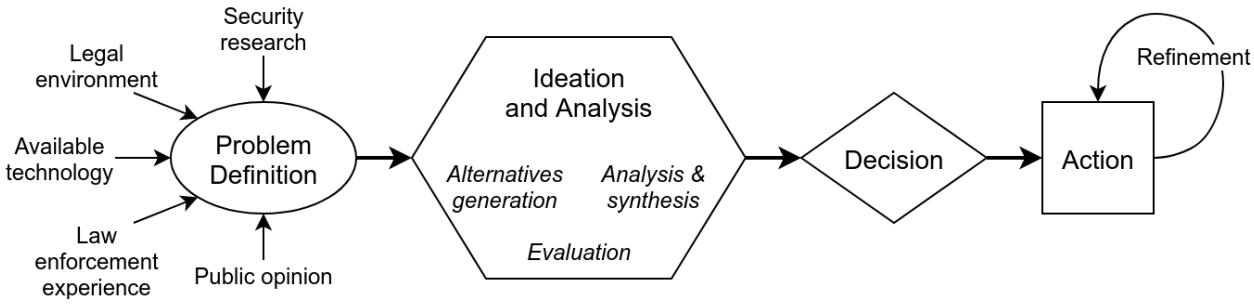

FIGURE 3.1 The Classical Analytic Method

3.2.2 Incrementalism

Incrementalism is an intuitive and iterative approach posed as an alternative to the classical analytic method. Incrementalism as a policymaking strategy is often referred to as "muddling through" from political scientist Charles Lindblom's classic paper defining and defending the approach [96]. Written before Rittel developed the idea of "wicked problems," Lindblom nonetheless identified many of the same shortcomings of the classical method and sought to formalize the process policymakers were already often using.

Lindblom's process of "muddling through" operates by taking successive steps chosen through comparative analysis. The alternatives selected for comparison must be defined relative to the status quo and must be close enough to one another that they can be analyzed on the margin. This is done due to (a) practical necessity, due to the inability to predict policy outcomes, and (b) out of political realism, as non-incremental changes are usually politically impossible to impose in a democratic system [96]. The formality of the process varies; policymakers may use this method consciously, with considerable comparative analysis, or unconsciously, led by intuition. Figure 3.2 illustrates this method.

Incrementalism has several advantages over the classical analytic method for handling wicked problems. It is rooted in realism about the limits of rational analysis. It accepts that the problem will not be conclusively solved. Instead, it emphasizes iteration: "Policy is not made once and for all; it is made and re-made endlessly. Policy-making is a process of successive ap-

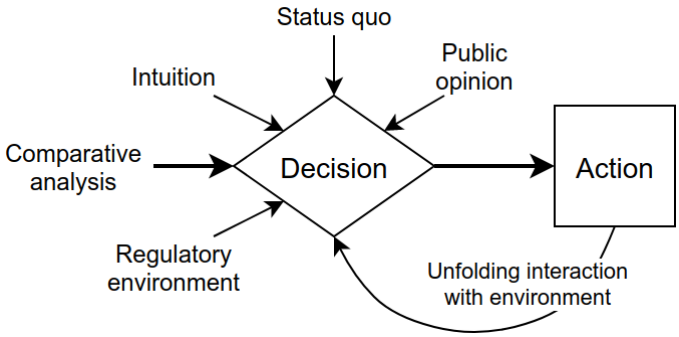

FIGURE 3.2 Incrementalism

proximation to some desired objectives in which what is desired itself continues to change under reconsideration" [96]. Most importantly, it eschews the linear flow from problem definition to alternatives analysis out of respect that the problem definition is not self-contained. Lindblom argues that policy ends and means are interlinked, eventually concluding:

> As to whether the attempt to clarify objectives in advance of policy selection is more or less rational than the close intertwining of marginal evaluation and empirical analysis, the principal difference established is that for complex [i.e., wicked] problems the first is impossible and irrelevant, and the second is both possible and relevant. The second is possible because the administrator need not try to analyze any values except the values by which alternative policies differ and need not be concerned with them except as they differ marginally. His need for information on values or objectives is drastically reduced as compared with the root [i.e., classical analytic] method; and his capacity for grasping, comprehending, and relating values to one another is not strained beyond the breaking point. [96]

Despite its strengths, incrementalism also has weaknesses in its ability to address wicked problems. Its main weakness is the absence of high level strategic analysis. Incrementalism is incapable of drastic change, which is sometimes necessary. By Lindblom's admission, it lacks a safeguard for consideration of all relevant values and may "overlook excellent policies for no other reason than that they are not suggested by the chain of successive policy steps leading up

to the present" [96]. Analysis based only on the present status quo can result in messy policy that pleases no one—"As Lindblom's sobriquet suggests, it often [leads] to a considerable muddle" [80]. Application of the Computer Fraud and Abuse Act is one such muddle [97].

Unfortunately, one cannot simply add high level strategic analysis to the incrementalist method by including the past in its analysis. Incrementalism relies on simplifying analysis by limiting it to marginal differences to a given baseline. If one tries to be a "strategic incrementalist" by looking into the past, they still have to choose a baseline from which to perform analysis. This approach is susceptible to two weaknesses in baseline-based reasoning that Rozenshtein describes in his analysis of EA as a wicked problem [2]. First, the choice of baseline is arbitrary, yet heavily colors analysis:

> Both the government and its critics have operated from the status-quo baseline, though from opposite directions. For the government, the relevant baseline is recent history—specifically, right before companies like Apple and WhatsApp encrypted their products. From this baseline, the government's ability to surveil has diminished. For critics of government surveillance, the relevant baseline is the pre-digital age, before smartphones and social media vastly expanded the government's surveillance capabilities. From this baseline, the technological changes underlying the "going dark" problem are mere blips on the otherwise rocketing growth of the surveillance state. [2]

Second, unlike legal baselines, policy baselines do not carry normative force. Constant changes in the underlying situation mean that even optimal policy in the past is not necessarily desirable in the present. Due to these weaknesses, applying incrementalist methods at the strategic level does not work.

A final weakness in incrementalism is its assumption of basic agreement and political stability. The method works by limiting analysis to marginal comparisons of broadly similar and familiar proposals. Proposals that differ widely from one another or the status quo are considered irrelevant because the debating parties both share the same general goals and lack the ability

to unilaterally impose their will. Rather a symptom of present circumstances (see Section 2.2.4) than an inherent weakness in the incrementalist approach, both of these assumptions are incorrect.

3.2.3 Lessons

The classical analytic method and incrementalism are not the only styles of policymaking. They represent perhaps two extremes on a spectrum of rational planning and intuitive "muddling." Both have strengths and weaknesses. One may intuit that a reasonable strategy is the selective use of both approaches according to the situation, and indeed this has been formally suggested [98]. However, even a combination of these methods does not suit all classes of wicked problems. Is a problem tame? Use the classical analytic method. Is it wicked, but strategically under control and relatively non-controversial? Use incrementalism. What about when it is it wicked, lacks a strategic response, and is highly controversial?

Wicked problems were earlier described as a tangle of contributing subproblems. Using this characterization, dealing with a wicked problem requires disentangling the web, identifying the tame subproblems, and developing agreeable strategies for the irreducibly wicked subproblems. Once that is done, we can rationally analyze and increment our way to resolution. There is no handbook for how to do this, but several sources offer advice.

- **Reject Easy Answers**

  Easy answers, or any solutions that artificially tame the problem, will not bring the matter under control. While by definition there is no solution that will truly solve a wicked problem, easy answers deliberately emphasize one value to the exclusion of others. Because they neglect the root issues, solutions based on easy answers produce unintended consequences and chaos in those neglected areas [93].

- **Bring Everyone to the Table**

  Including every relevant group is important for two reasons. First, because information is "uncertain and diffuse," generating an accurate problem statement requires diverse input [2]. Second, for incrementalism to work on the irreducibly wicked roots of the problem, there needs to be some degree of consensus on overall strategy. Consensus building is not easy among groups with differing values and priorities, but it is impossible without each group being represented.

- **Unite Problem Definition and Analysis Steps**

  The failures of the classical analytic method and incrementalism reveal that we must be able to think strategically while respecting the non-linear nature of wicked problems. One must use the high level, holistic view of the classical approach while intertwining the problem definition and analysis steps as in the incrementalist approach. In practice, this means that the collective understanding of the problem and potential solutions must co-evolve. As Rittel puts it, "The systems-approach 'of the first generation' [i.e., classical analysis] is inadequate for dealing with wicked-problems. Approaches of the 'second generation' should be based on a model of planning as an argumentative process in the course of which an image of the problem and of the solution emerges gradually among the participants, as a product of incessant judgment, subjected to critical argument" [1].

- **Embrace Flexible, Risk-Based Solutions**

  Wicked problems' potential solutions cannot be comprehensively evaluated before or even after implementation and each action (or decision not to act) has irreversible effects. Proposals must therefore be agile. All decisions involve unknowns, but risk- and uncertainty-management strategies can optimize the expected outcome and maximize the worst outcome [99].

- **Focus Discussion around Concrete Proposals**

  Focusing on concrete proposals follows partially from the previous lesson—problem definition and analysis are combined precisely because the problem definition depends on the nature of proposed solutions. But this advice deserves emphasis for another reason: consensus is easier to achieve for concrete proposals. Debate in the abstract can rage endlessly, as groups are bound to disagree due to their conflicting values and priorities. However, Lindblom writes encouragingly about "the ease with which individuals of different ideologies often can agree on concrete policy" in an example about congressional compromise. He goes on to say, "Labor mediators report a similar phenomenon: the contestants cannot agree on criteria for settling their disputes but can agree on specific proposals. Similarly, when one administrator's objective turns out to be another's means, they often can agree on policy" [96].

3.3 Proposal: The OODA Loop for Wicked Problems

The discussion above describes the inability of well-established methods of policymaking to address wicked problems and lessons for shaping a better method. Here, I propose a modified OODA Loop as an alternative policymaking model.

The *Observe-Orient-Decide-Act* Loop (OODA Loop) was developed by Air Force Colonel John Boyd as a description of a successful strategy for countering opponents in real-time combat [100]. Boyd created it in the context of military strategy, but its ideas have penetrated many other sectors, including cybersecurity, where it serves as a model for structuring incident response [101]. The model emphasizes fast cycle times and "getting inside" your opponent's loop as a means of overcoming raw power with speed and agility. It is illustrated in Figure 3.3.

The OODA Loop serves well as a model for contending with wicked problems because it has the correct fundamental structure. It corresponds closely to the classical analytic method steps of problem definition (orientation), ideation and analysis (orientation), decision, and action; how-

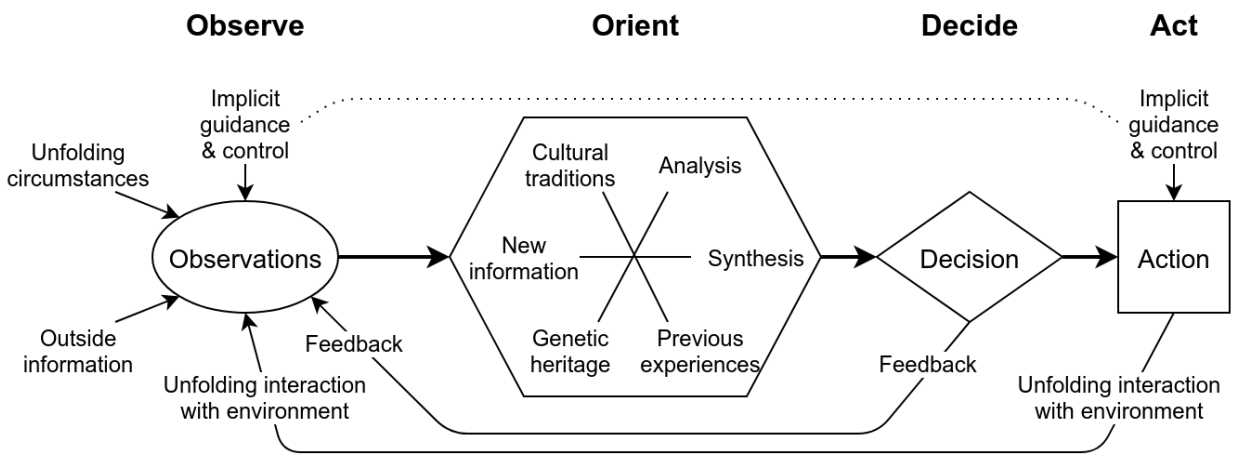

FIGURE 3.3 The OODA Loop

ever, it also emphasizes incrementalism's iteration and feedback. Additionally, while policy-making does not share the pace of real-time combat, this metaphor holds true in other ways. In both cases, one faces an unpredictable opponent in a dynamic environment in which every action counts. We cannot overpower wicked problems through force of reason, but perhaps we can through feedback and agility.

The OODA Loop does need one modification in order to suit wicked problems. Because the problem definition step and analysis step depend on one another, they must be joined. This is Rittel's "argumentative process in the course of which an image of the problem and of the solution emerges gradually" [1], illustrated in Figure 3.4 as a cycle of "collaborative debate" between observation and orientation. The modified OODA Loop incorporates each of the lessons from Section 3.2.3.

3.4 Summary

Traditional policymaking typically follows either (a) a rational approach rooted in the scientific method, aiming to be thorough and complete, or (b) an intuitional approach rooted in evolutionary trial and error, humbly aiming only to take steps in the right direction. Both approaches have strengths, but neither is suited to the complex and controversial nature of wicked problems.

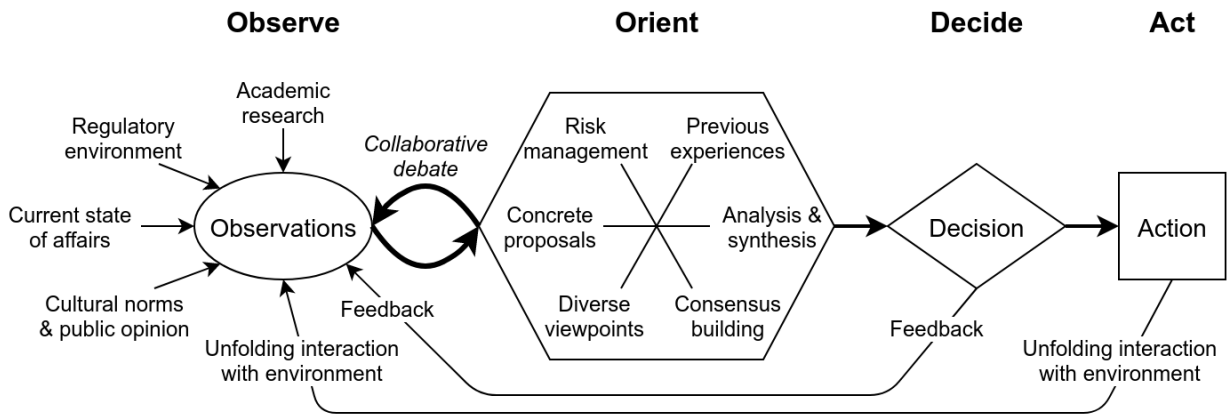

FIGURE 3.4 The OODA Loop for Wicked Problems

The strategy proposed here relies on the goodwill participation of all parties who engage in on-going research and debate that rejects easy answers, encourages flexible risk-based solutions, and crystallizes discussion around specific proposals. The result of a single iteration is a bit more clarity and a small step forward. The result of many iterations is the breakdown of the problem into subproblems—some tame and inevitably some still wicked. The tame subproblems can be addressed with the classical analytic method, and the wicked subproblems, by now restrained under a sound and agreeable strategy, can be addressed with incrementalism.

This process is demonstrated in Figure 3.5. An out-of-control problem (represented by the large storm) is confronted in this diagram. Several iterations of the OODA Loop gradually diminish its size. This is achieved by spinning out tame problems (represented by puzzle pieces) which are addressed with classical analysis and wicked but restrained problems (represented by small storms) which are controlled by incrementalism.

It is important to note that the same wicked problem is never faced twice, since each one is by definition, unique. However, changes in technology, culture, and current affairs may render the current strategy insufficient and require the process to start again. It has been said that history does not repeat itself, but it rhymes. Wicked problems are the same. Past solutions cannot be used in the future, but lessons learned can be.

In the context of encryption and EA, this means that the outcome of the first crypto war

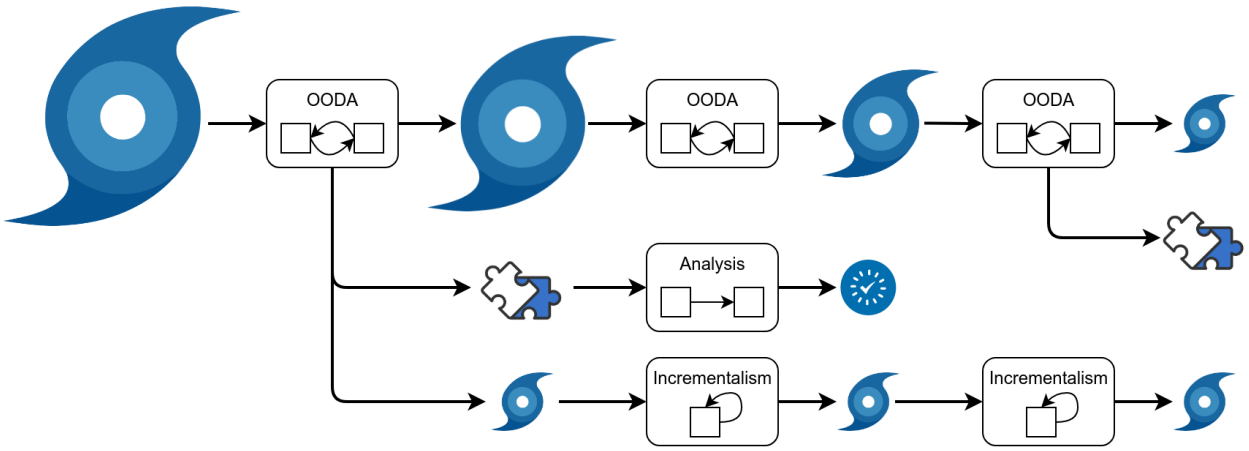

FIGURE 3.5 Using the OODA Loop to Tackle Wicked Problems

doesn't hold precedential power over the debate in the second. It means that it is legitimate to re-raise questions about the role technology plays in society. Hard-line rhetoric doesn't help [10] [48], but sincere appeals do [8] [6] [102]. Collaborative efforts involving government, technical, and civil liberties representatives are even better [103] [45]. Specific proposals around which groups can center discussion are also necessary. This is true whether they specify a particular form of EA or (perhaps especially) if they offer an alternative [21] [59] [54].

I apply this strategy in the remainder of the thesis. Chapter 5 documents the debate in depth and Chapter 6 defines a threat model against which I analyze a specific EA proposal.

CHAPTER 4

Analysis Tools

Encryption policy arguments and exceptional access threat models are complex. Argument maps and data flow diagrams are two methodological tools that can be used to structure analysis and manage complexity. This chapter introduces these tools and their syntax, which will be used in Chapter 5 and Chapter 6.

4.1 Argument Maps

In order to advance the EA discussion, it is necessary to organize the many different arguments in a cohesive manner. This thesis uses argument maps to do so. Argument maps are graphical representations of the logical structures and relationships between statements, premises, and conclusions. They originated from the same research as the idea of wicked problems. Though formal research on the technique is sparse, argument maps have proven helpful in simplifying complex arguments regarding wicked problems and in facilitating debate [104]. This is because they slow down discussion, depersonalize conflict, and lend structure and rhythm to meetings [105]. They are therefore useful as a tool for conducting the OODA Loop model's "collaborative debate" step.

Argument mapping tools originated in 1970 with text-based issue-based information systems (IBISs) [106]. Graphical software mapping tools include the now-defunct gIBIS [107] and Compendium [105]. Argdown is a recent tool that generates graphical argument maps from structures specified in a Markdown-based language [108]. Argdown is used in Chapter 5 to analyze the arguments used in the EA debate.

Figure 4.1 shows the basic structure of arguments. Statements can take the form of positions, values, and assertions. The "Proposals," "Statements," "Fallacies," and "Values" in the figure are classes of statements in this sense. The color of a statement's border indicates the class to which it belongs. Arguments are premise-conclusion structures that relate to statements; they are classified as "anti-EA," "pro-EA," "neutral," or "fallacious." An argument's class is distinguished

by the color of its solid background. Statements and arguments may support, attack, or undercut one another. Green arrows represent supporting relationships; red arrows, attacking; and purple arrows, undercutting.

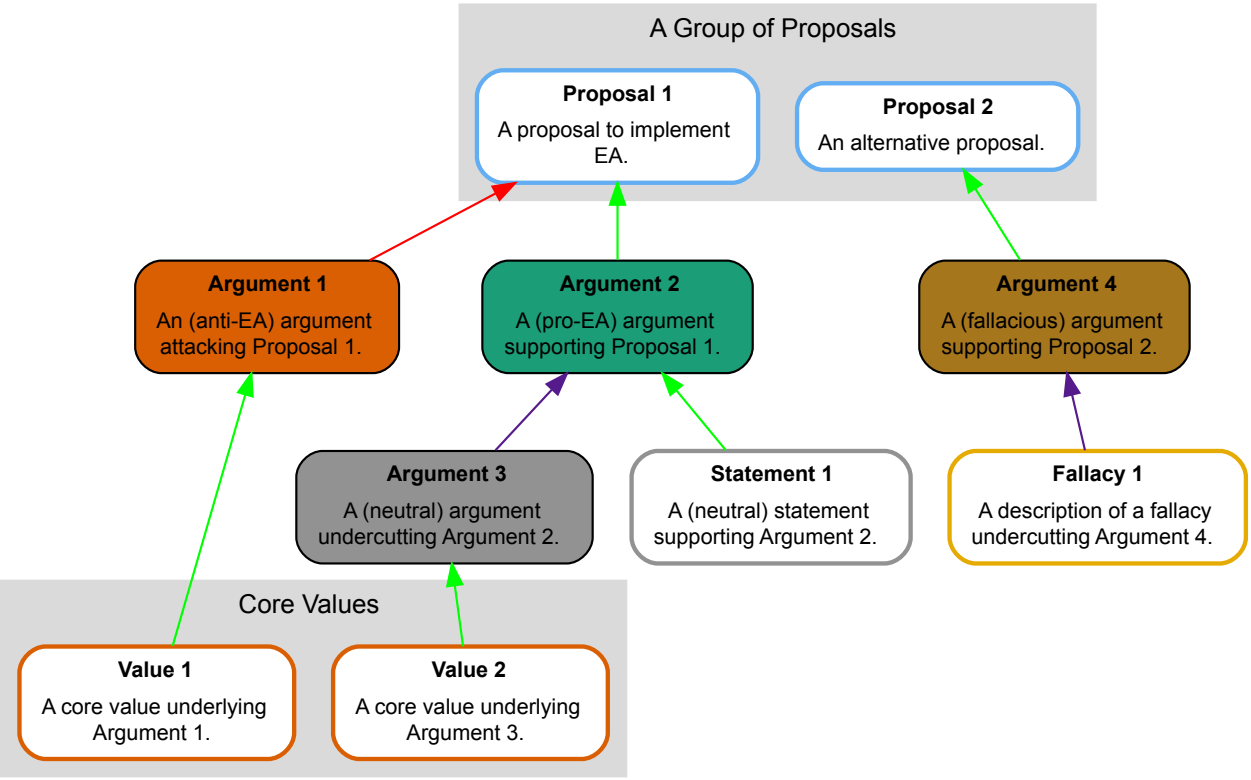

FIGURE 4.1 A demonstrative example of argument maps with Argdown

4.2 Threat Modeling with Data Flow Diagrams

Threat modeling is an important step in analyzing the security at the systems level. Models abstract away fine details and focus on the architecture, processes, and dataflows in a system. They assist in the understanding of current systems and the prevention of problems in new systems, both of which are important when facing the prospect of designing an EA mechanism built on top of a complex and aging technology stack.

Threat modeling begins with the questions, “What are you building?” and “What can go wrong?” [13]. Accurately answering the first question is crucial, particularly for the field of

cryptography, which hinges on precise definitions of security requirements [109]. The answer to the second question depends on the types of attackers under consideration and determines the scope of threats to be considered. "What are you building?" hasn't been asked enough in the current phase of the EA debate, and "What can go wrong?" cannot be faithfully answered without knowing what is being built.

Data flow diagrams (DFDs) were designed to address these questions. DFDs feature processes, data flows, data stores, and external entities. DFDs are well-suited for threat modeling because security vulnerabilities tend to follow data flow, not control flow [13]. They are particularly well-suited for EA, as data privacy is of primary concern. Figure 4.2 shows the basic elements of a DFD of a simplified Diffie-Hellman key exchange.

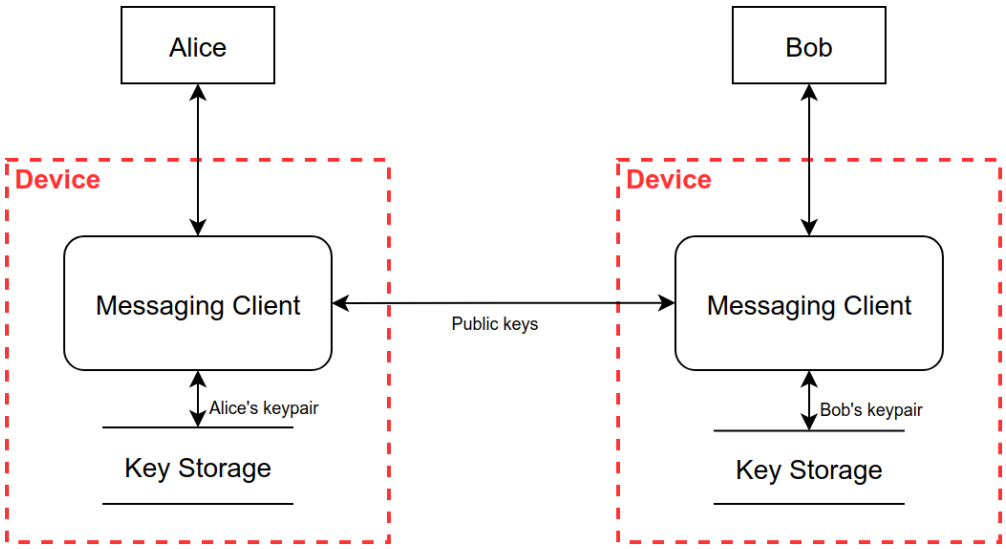

FIGURE 4.2 A DFD for a simplified Diffie-Hellman key exchange

DFDs show what data is transferred via labels on the flows. However, labels can be insufficient in complex DFDs, and the method has no syntax for computation or cryptographic protocols. In order to maximize their communicative ability in the context of encryption and exceptional access schemes, I introduce the additional syntax show in Figure 4.3.

The new syntax illustrates the data in more detail as it is stored, transferred, and operated on. By illustrating the data itself, it eliminates the need for labels on lines and can be used to communicate entire protocols in a single diagram. Figure 4.4 contains the full set of symbols. Chapter 6

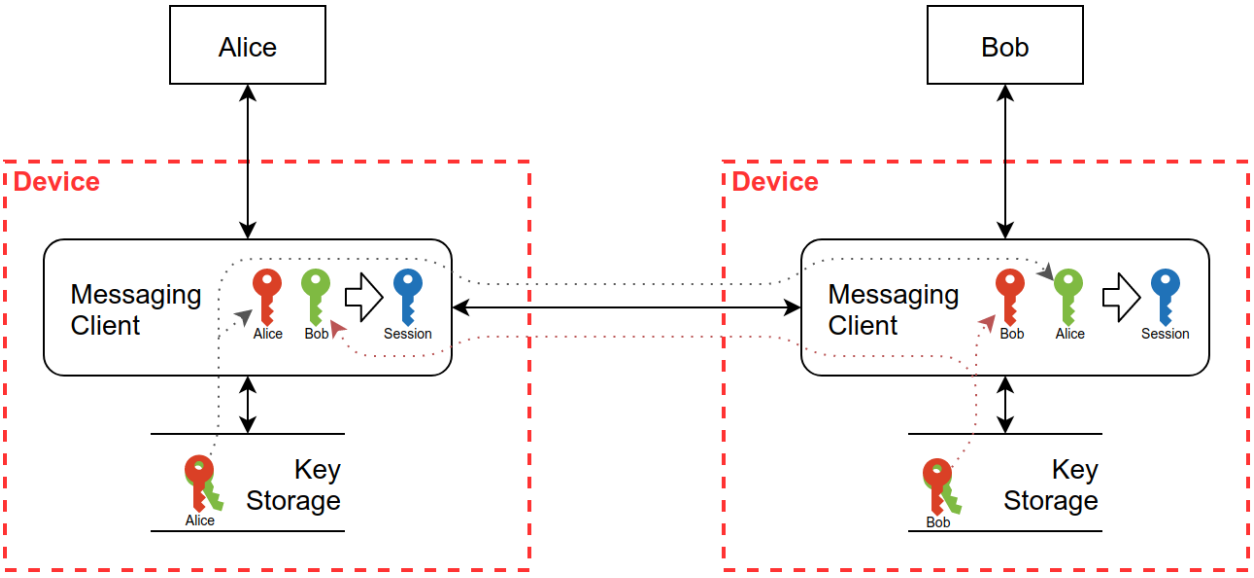

FIGURE 4.3 A Diffie-Hellman key exchange illustrated with additional syntax

includes DFDs in this style to analyze threats that EA would introduce.

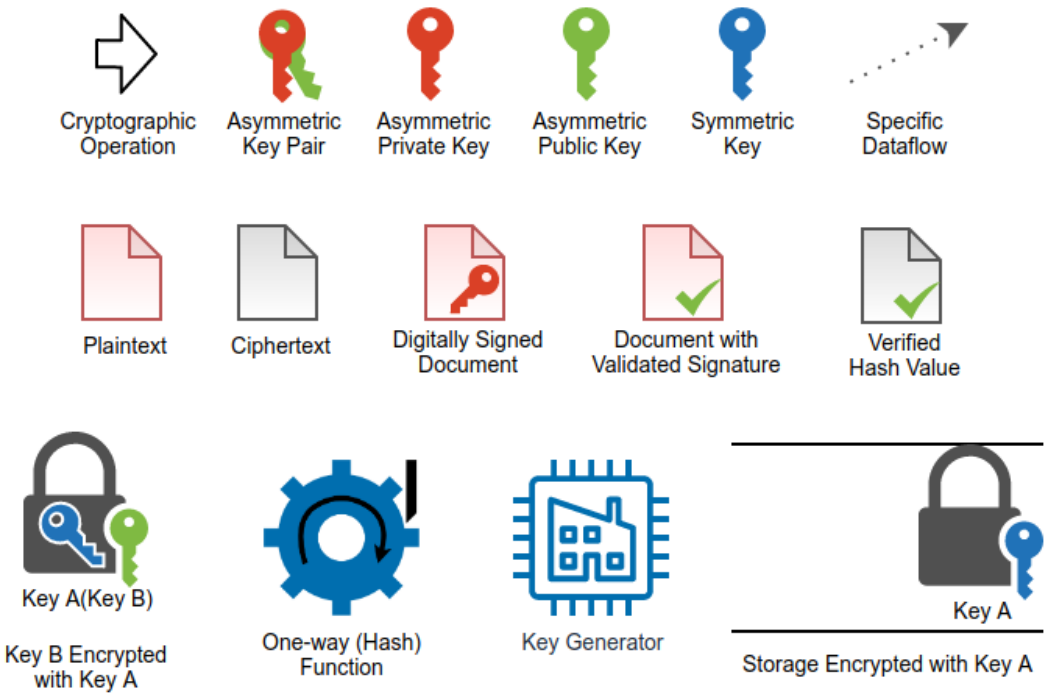

FIGURE 4.4 Expanded set of DFD symbols

CHAPTER 5

EA Debate Arguments

This chapter will analyze the encryption debate using argument maps. The maps facilitate comprehension of the debate, but there are two important shortcomings of the maps presented here. First, argument maps should be used simply as tools in the collaborative pursuit of the problem definition and solution. Maps assembled from research are not a replacement for debate arising from live discussion. Second, argument maps may deceptively portray the strength of an argument. Argument nodes do not indicate their strength or validity. If ten unsound arguments were presented against one indisputable argument, the side with more arguments would, regardless of the arguments' integrity, appear stronger. With those qualifications in mind, let us begin by examining the factors at the center of the conflict.

5.1 Contributing Factors

Figure 5.1 maps the central arguments in the EA debate. As previously stated, encryption's dual contributions to information security and radical privacy are central to the debate. Of course, there is only conflict when radical privacy is perceived as a negative. The right to privacy is both a strongly held value and an enshrined legal principle. Many use privacy concerns to argue that EA is socially undesirable. The Snowden revelations [36] unveiled the scale of privacy-eroding U.S. government surveillance enabled by technological changes, terrorism-motivated policies, and weak oversight [34]. Privacy violations are an abstract concern to many, but for those most vulnerable, they are frighteningly concrete. For example, mobile phone surveillance malware enabled the Saudi government to capture and murder journalist Jamal Khashoggi for expressing dissent against the crown prince [110]. At a societal level, the mere presence of surveillance changes behavior and suppresses free speech [111], and government violations of the law degrade institutional trust.

Law enforcement argues that encryption handcuffs its investigational capacity. The FBI brands strong encryption as "warrant-proof" and states that "the government often cannot ob-

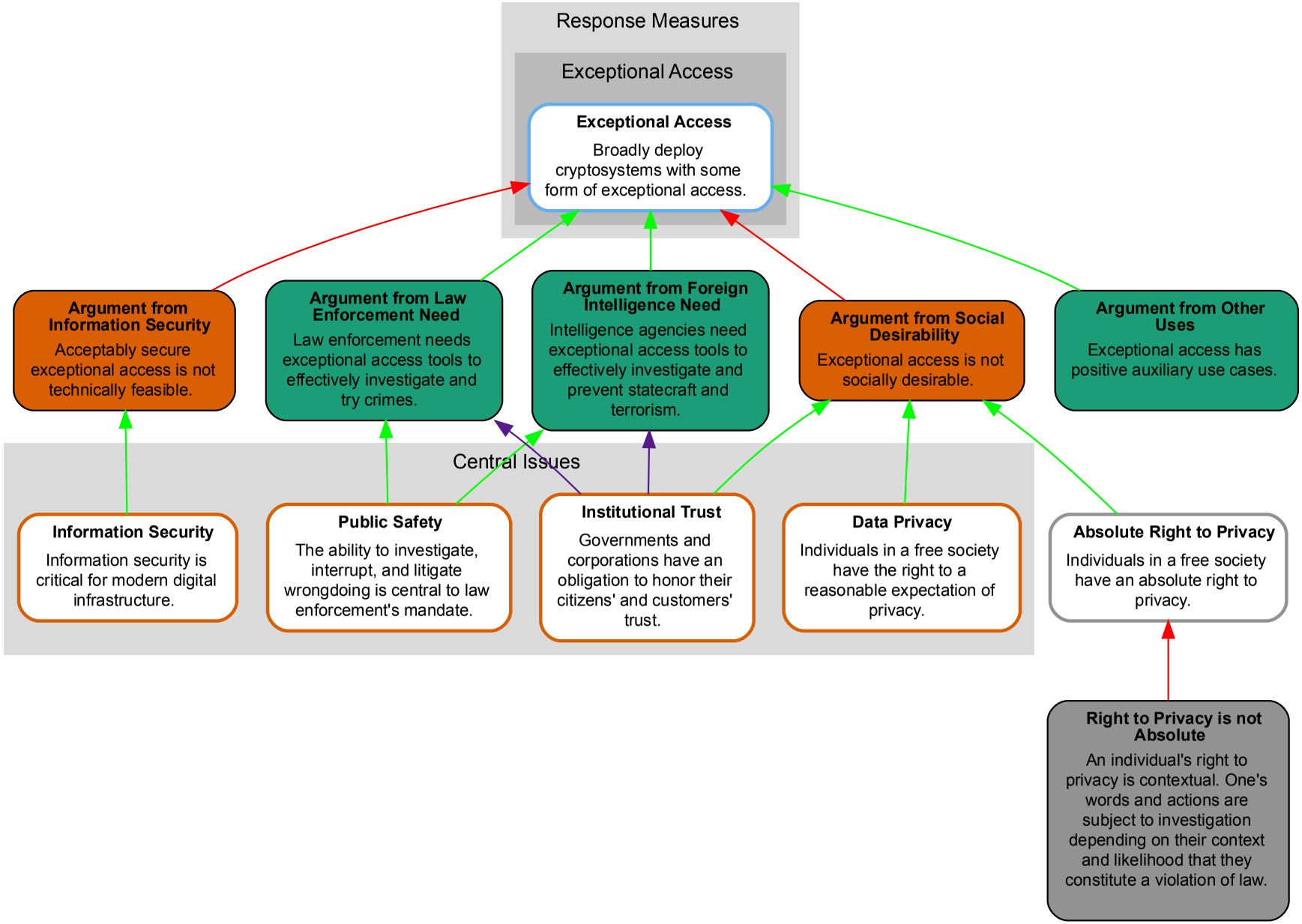

FIGURE 5.1 Contributing Factors to the EA Debate

tain the electronic evidence necessary to investigate and prosecute threats to public and national safety" [112]. The pro-EA argument is typically rooted in public safety: encryption makes it too difficult for investigators to access the evidence needed to catch and convict law-breakers. Five-eyes nations have regularly published joint statements expressing their frustration with encryption [5] [113]. They were joined in 2020 by India and Japan in a statement emphasizing the growing danger of CSAM [6]. Child pornography is one of the original Four Horsemen used to scare people into supporting backdoors [44], but it is also a problem growing to astonishing proportions. A 2019 investigation by the *New York Times* quoted a law officer's estimate that 400,000 New Jerseyans, more than 4% of the state's population, have violated child exploitation material laws [4].

Unfortunately, these shocking claims have not been independently confirmed with hard data. Intelligence agencies have historically misrepresented statistics and overstepped their bounds [114] [34]. This undercuts their claims that they need EA and has diminished institutional trust. For example, the FBI has already been found to exaggerate the number of mobile devices it could not access due to device encryption [115]. As Rozenshtein points out, "It is impossible to know the precise extent to which encryption frustrates law-enforcement investigations, both because law-enforcement agencies are only beginning to collect accurate statistics, and because one can never be sure of how an investigation would have proceeded in the absence of encryption" [2]. However, it is still crucial to have an accurate depiction of the problem in order to come to justified and helpful solutions. This argument is analyzed further in the next section.

Information security is the remaining central issue in the debate. As described in Section 2.1, cryptography plays a foundational role in nearly every aspect of security. Past EA regulation efforts sought to compromise the cryptographic foundations of encryption; however, this is seen as too risky today. Section 2.3 introduced several alternative technical approaches to EA, but experts still emphasize that current systems cannot securely provide the level of access law enforcement asks for [8] [116]. Security was an afterthought in early computing and networking designs. The field of cybersecurity is still equal parts art and science; mandated EA would put a

heavy burden on a field still finding its legs.

Finally, it is arguable that EA could have positive alternative applications. It could enable malware scanning, password recovery, or administrator access in a business setting. Typically these applications have other solutions, however, and unnecessary requirements would weaken EA systems.

5.2 Going Dark vs. The Golden Age

Much of the disconnect between government and the technical community is the result of disagreement over whether law enforcement has *too little* or *too much* access to data. The argument for *too little* is well-represented by proponent former FBI Director James Comey in his 2014 speech titled "Going Dark" [7] (though he did not coin the phrase [117]). The argument is presented in Figure 5.2.

According to the "Going Dark" argument, privacy and safety are both desirable goods, but they conflict with one another; therefore, they must be balanced. Individuals must sacrifice some of their personal good of privacy to allow for the public good of safety. Widespread encryption tips the scales too far towards privacy, upsetting the balance that existed before. EA restores the balance and enables law enforcement agencies to fulfill their duty to protect the public.

The "Going Dark" argument has a few shortcomings. It oversimplifies the relationship between privacy and safety by depicting it as a zero-sum conflict. In reality, privacy does not always diminish safety, but sometimes enhances safety. For example, data privacy makes crimes such as stalking and identity theft more difficult. The "Going Dark" argument also categorizes privacy as a personal good and safety as a public good. However, privacy can also be a public good when it counters mass surveillance. This argument is explored more deeply in the "Golden Age for Surveillance" map.

Most importantly, the "Going Dark" argument relies on the premise that law enforcement investigations fail due to encryption. As described in Section 5.1, there is no conclusive data regarding the extent to which encryption is to blame for failed cases. The highest-profile case

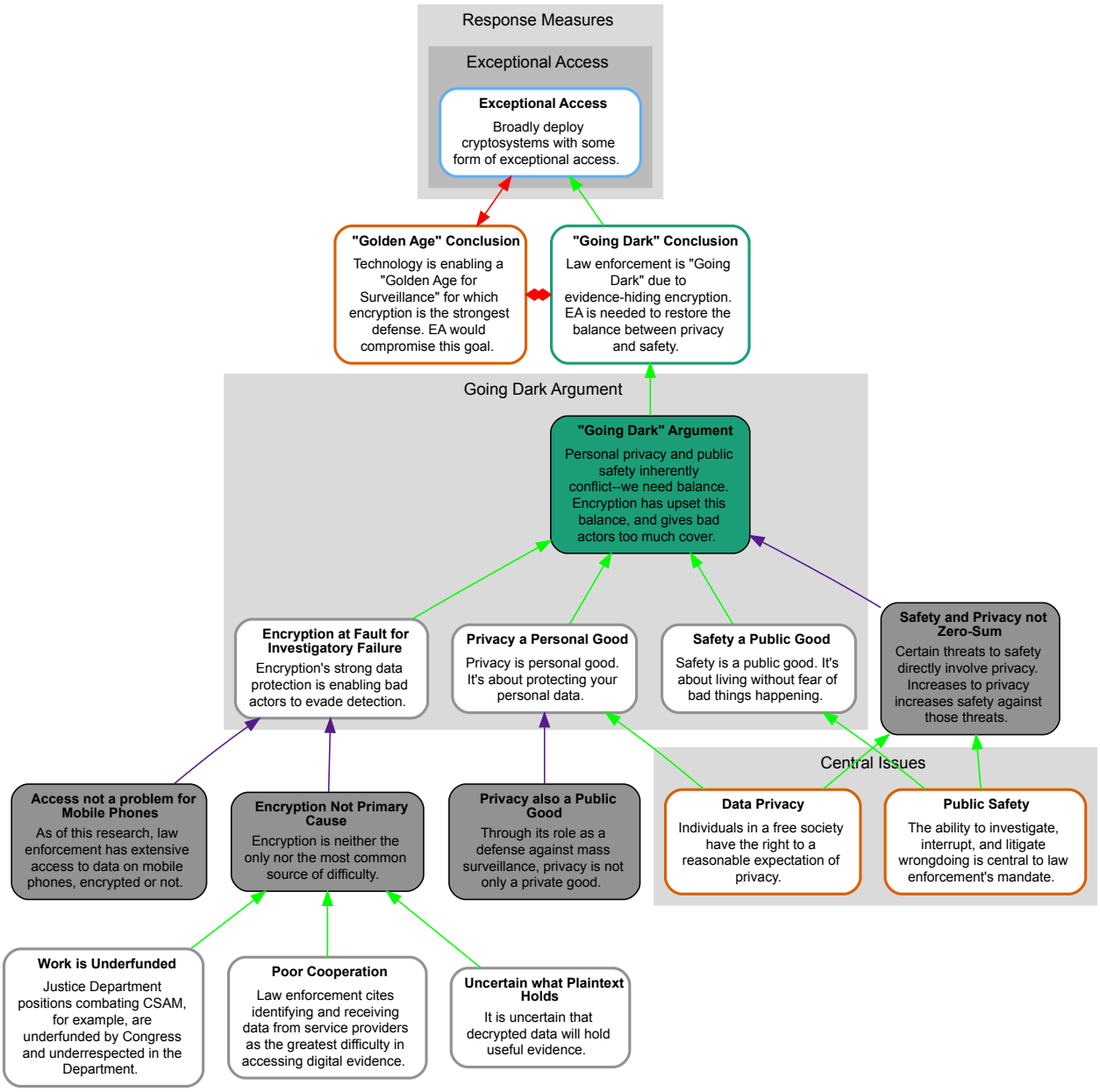

FIGURE 5.2 A "Going Dark" Argument Map

of the second crypto war, Apple vs. FBI, ended when the FBI broke into the phone and found nothing of value. Tellingly, the examples cited in Comey's 2014 speech were not cases in which encryption inhibited investigations, but were cases in which encryption *could have* inhibited investigations, had it been a factor. [7]. More recently, a 2020 report titled "Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones" revealed that current

hacking tools are stronger than the defenses provided by mobile device encryption and that law enforcement is actually able to extract data from nearly every mobile phone on the market [118]. The lack of conclusive data showing the extent that encryption hinders investigations is a weakness of the "Going Dark" argument.

However, lack of evidence for an argument does not prove that it is incorrect. Because law enforcement has the data, the burden of proof is on them—they must show that encryption is causing investigatory failure. Unfortunately, in most cases, it is impossible to know what would have happened without the interference of encryption. Inability to gather data from controlled tests is a characteristic of wicked problems. When controlled settings are unachievable, another way to gather data is by observing naturally-occurring conditions in which everything but the variable of interest are constant. These conditions exist for encryption in the messaging application ecosystem. Messaging applications WhatsApp, Facebook Messenger, and Telegram all have large user bases and similar features. Among these services, only Facebook Messenger does not employ E2EE. Globally, Facebook Messenger has approximately 20% market share as measured by active monthly users [119] but accounts for 65% of CSAM reports [4]. This indicates that encryption does indeed affect investigations.

Encryption is not the only challenge that law enforcement faces with digital evidence. A 2018 study found that identifying and cooperating with service providers through existing legal frameworks were even greater challenges [120]. The report, titled "Low-Hanging Fruit," also lists resource limitations and poor training as top issues. Indeed, many current initiatives are underfunded. The *New York Times*' 2019 investigation into CSAM uncovered a chronic lack of commitment from government initiatives [4]. Major legislation passed in 2008, but has been funded at only 50% of authorized levels; a commissioned Justice Department task force has produced only two of five biennial reports; and a senior executive position within the Justice Department to target CSAM was never created. Federal entities aiming to improve training and coordination between law enforcement and industry are similarly underfunded [120].

The argument for law enforcement having *too much* access to data claims that law enforce-

ment is not "Going Dark"; rather, they are experiencing the "Golden Age for Surveillance" [117]. This argument posits that although encryption makes certain data completely unaccessible, technological change on the whole has given authorities much more digital evidence than encryption has taken away. Paired with the dangers of mass surveillance, encryption is a necessary defense. EA would compromise encryption's defense against mass surveillance, and must therefore be opposed. The argument is mapped in Figure 5.3.

The "Golden Age" argument focuses on surveillance, its undesirability, and technology's role in it. Cryptographer Phillip Rogaway writes at length about the negative impacts of mass surveillance in his essay "The Moral Character of Cryptographic Work" [111]. Rogaway asserts that "pervasive collection *itself* chills free-speech and threatens liberal democracy." He argues that surveillance is fundamentally a tool of power, and for this reason it should be resisted. Though power from the people, created through representative political process, is valid, clear abuses have undercut confidence in these institutions.

After establishing the danger of surveillance, the argument notes that technology has increased the government's surveillance abilities. This statement is supported by strong evidence. In Comey's "Going Dark" speech, it was digital evidence which would not have existed twenty years ago that cracked each case [7]. Encryption is one of the only privacy-saving technologies to emerge alongside the boom in privacy-eroding technologies. Opting out of the technological boom is possible for some, but is not a realistic option for society as a whole. Due to the dangers of mass surveillance, encryption must be embraced.

While stronger than the "Going Dark" argument, the "Golden Age for Surveillance" argument suffers from a significant flaw. It focuses on the abilities and dangers of agencies like the NSA while ignoring the problems of resource-strapped local, state, and federal law enforcement. It is obvious that the amount of digital evidence is increasing. However, as seen in "Going Dark" argument, law enforcement often struggles with digital evidence for reasons unrelated to encryption. Exacerbating the problem for justice system is the "tech effect," which refers to jurors' increased expectations of digital evidence in cases where they suspect it exists [121].

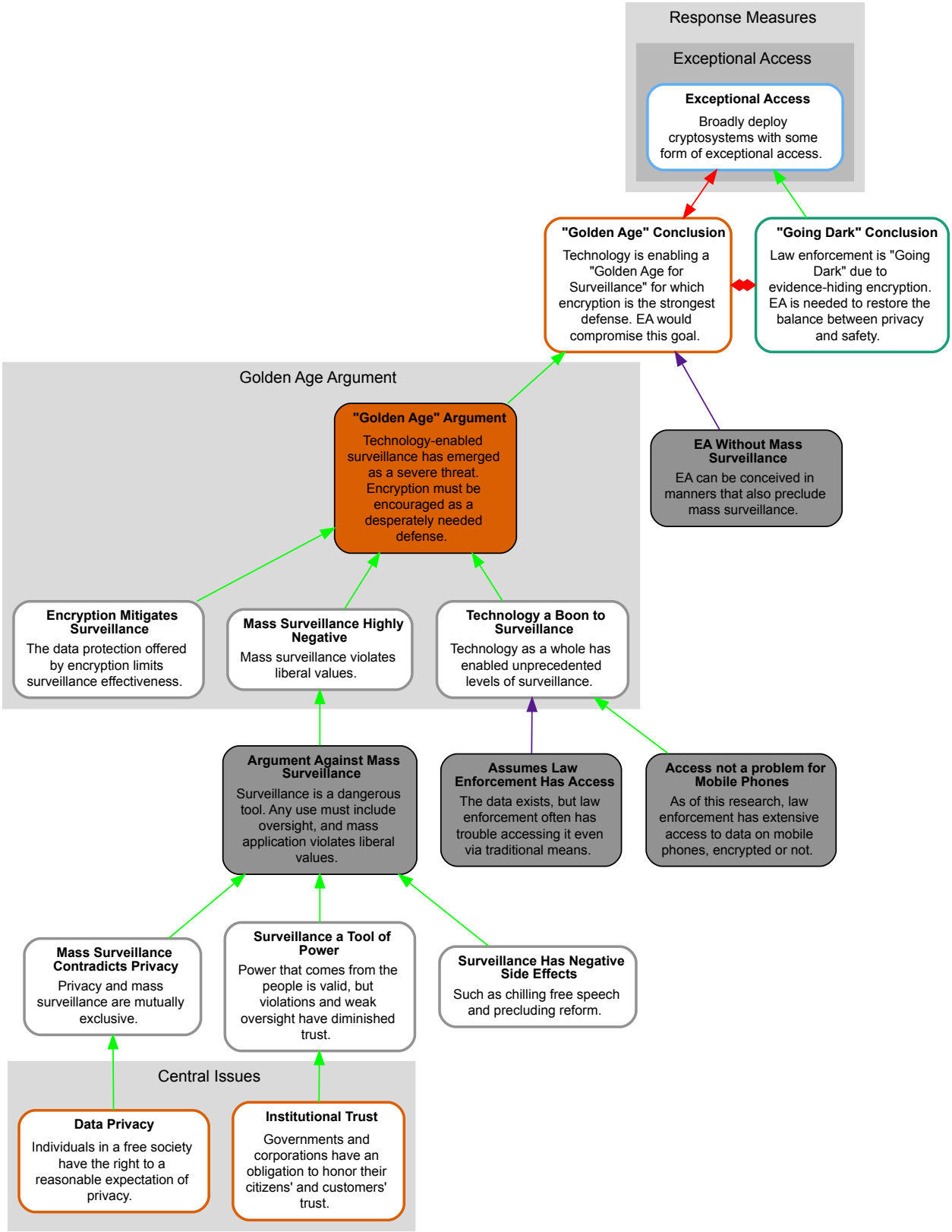

FIGURE 5.3 A "Golden Age for Surveillance" Argument Map

Still, law enforcement's inability to access the tools of mass surveillance cannot be taken for granted. It will likely change—they already have access to mobile devices. A more conservative criticism of the "Golden Age" argument rests in the fact that EA without mass surveillance is conceivable. EA implementations that enable law enforcement while thwarting mass surveillance subvert most of the "Golden Age" argument. EA proposals with these aims will be explored in Section 5.5.

5.3 Eliminating Fallacious Arguments

Using argument maps to analyze debates allows for consideration of opposing arguments. Part of that consideration includes identifying and eliminating fallacious arguments. In heated partisan debates, fallacious arguments spread easily. Figure 5.4 shows those most commonly used in the encryption and EA debate.

The map begins with fallacious arguments used to attack EA. The first is the most common: "EA is a bad idea because backdoors are insecure." It appears on the map as a straw man argument due to the way the term "backdoor" is used. "Backdoor" is essentially technical shorthand for "insecure hack that should never be used in production"; when it is used as a basket term for all EA proposals, the audience is primed to consider them all ill-conceived and hopelessly dangerous. Thus, the arguer is presenting their opponent's argument for any degree of EA in the weakest possible fashion.

Another common argument is that implementing EA—or even researching it—inexorably moves tech policy down a slippery slope in which government demands will never be satisfied. This argument can be used to discourage those seeking a middle ground. Going too far and too fast is certainly dangerous, but it is both cynical and misleading to declare the permanent destruction of privacy as the inevitable end of EA research.

It is tempting to declare government requests for EA disingenuous due to their hypocritical behavior towards some of these issues. For example, if combatting CSAM is a government priority, why has Congress underfunded the laws it's passed, and why has the Justice Department

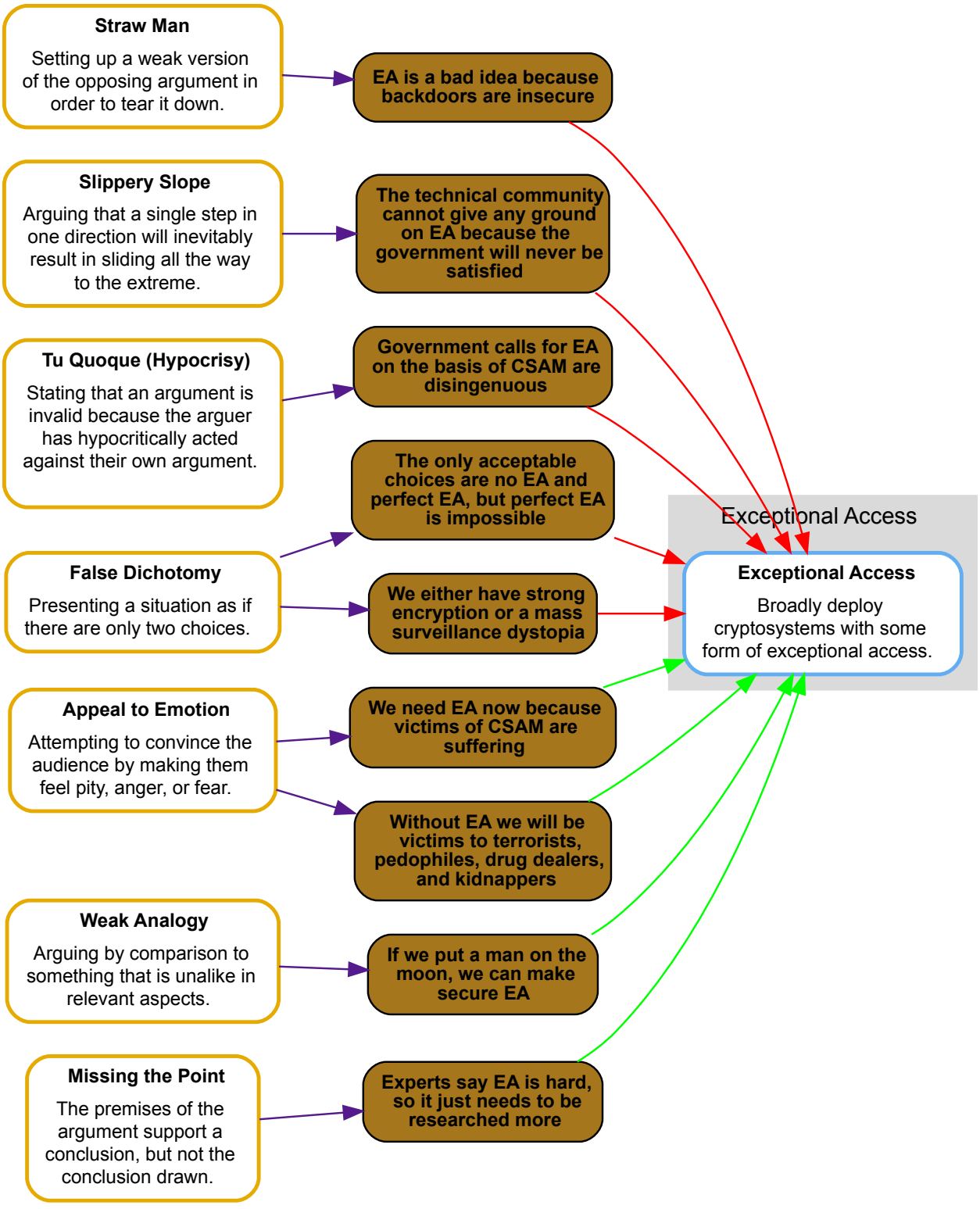

FIGURE 5.4 Fallacious Arguments of the EA Debate

understaffed its task force [4]? These questions demand answers, but they do not change the validity (or invalidity) of pro-EA arguments. The absence of government funding does not mean technical anti-CSAM measures are unnecessary.

The final two anti-EA fallacies are examples of false dichotomies; they present the situation as if there are only two options. Wicked problems have unlimited sets of potential responses, so reducing them to two is misleading. Arguers create a false dichotomy when they present either perfect EA or no EA at all as the only acceptable solutions. This leaves no room for risk-based approaches, the typical security strategy outside the realm of cryptography. Opponents of EA create another false dichotomy when they suggest that regulators must allow strong cryptography or we will live in a mass surveillance dystopia. This argument has elements of the "slippery slope" and appeal to emotion fallacies as well. Framing the situation in all-or-nothing terms reduces the chance of a successful collaborative debate.

Some arguments used to support EA rely on appeal to emotion. Politicians and law enforcement agents often argue for EA by appealing to pity for child abuse victims or appealing to fear of terrorists, drug dealers, and kidnappers. Public safety is a central issue in the debate. The technical community does take these concerns seriously [44]. These appeals become fallacious when they are used to manipulate the audience into supporting solutions incommensurate with the problems or to manipulate the audience into believing that the technical community does not care about these issues.

When experts argue against EA due to security challenges, some respond that since we put a man on the moon, we can surely create secure EA [122]. This is a weak analogy. The only similarity between the challenge of landing an astronaut on the moon and the challenge of building a cryptosystem with secure EA is that they are both difficult. Once the political commitment was made, the Apollo program solved mostly tame problems and had enormous government backing. Resolving the encryption debate has neither of these advantages. Many similar arguments comparing EA to other feats of technological progress suffer the same faults.

Lastly, government officials often portray EA as a problem that security experts simply have

not researched enough. If experts just "nerd harder," as some put it, they will be able to find a solution [40]. However, this notion ignores the conclusions of research done thus far. Encryption policy is a wicked problem for which tame, technical-only solutions will not work [2]. Even on the technical side, research has concluded that EA is easy from a purely cryptographic point of view. The interfaces between the cryptographic and human portions of the system pose the real difficulty [116] [8]. This may not be an area of strong academic inquiry, but to frame lack of technical research as the primary roadblock to encryption policy progress misses the point.

5.4 EA and Alternatives

The last four maps framed the debate, presented leading arguments, and identified fallacious arguments. The next map explores potential solutions. Figure 5.5 divides potential solutions into the categories of current capabilities, legal measures, and EA. Current capabilities can be implemented today, and include maintenance of the status quo and increasing investment in current programs. Legal measures require a change in the text or application of the law, but do not require fundamentally new technical capabilities. These include compelling passwords, which requires legal clarification, and sanctioning lawful hacking, which requires a strategic pivot and an oversight framework. (These non-EA approaches were first introduced in Section 2.3.3.) In this section, EA is compared to its alternatives. EA variations are compared in the next map.

It should be noted that the argument map format works best when it displays the debate surrounding just one conclusion or proposal. This allows adequate room for elaboration on points and counterpoints. When a map includes multiple conclusions or proposals, it becomes a tangled web of connections, leaving no room for additional detail. For the sake of brevity, this thesis compares EA's alternatives and variations in single maps. For a thorough discussion of both EA's alternatives and variations, see the National Academies of Sciences, Engineering, and Medicine's 2018 report titled *Decrypting the Encryption Debate: A Framework for Decision Makers* [103].

In Figure 5.5, response measures are considered according to five metrics. These metrics are

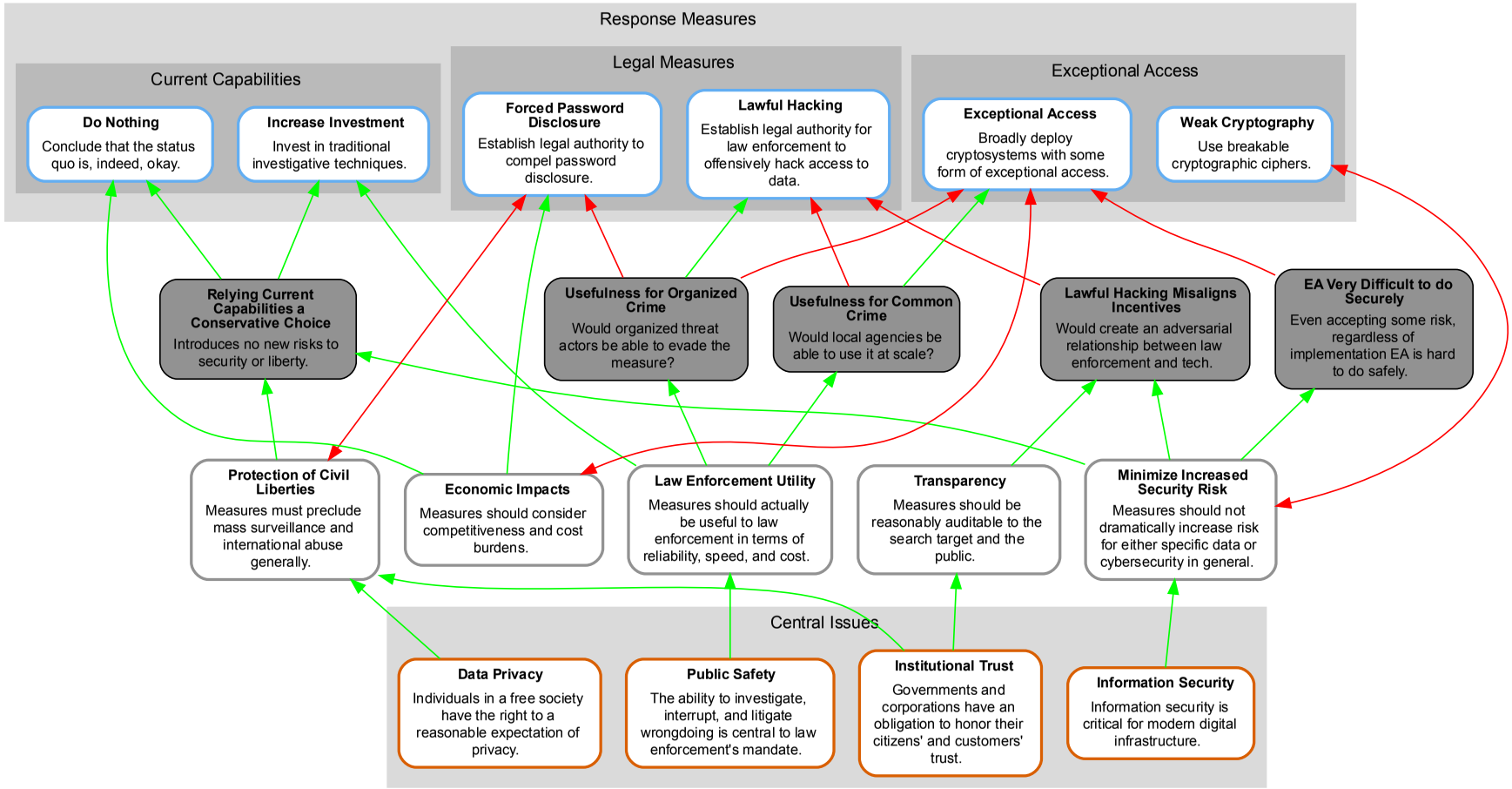

FIGURE 5.5 EA and its Alternatives

based on several sources, including two separate diverse committees gathered to analyze the encryption debate [103] [45] [109]. They also align closely to the four central issues of security, safety, privacy, and trust. The five metrics used to analyze response measures are (1) minimization of increased security risk, (2) utility to law enforcement, (3) protection of civil liberties—particularly important as after the analysis of the "Golden Age for Surveillance" argument—(4) transparency, and (5) economic impact. Economic impact is not as central an issue as the others, but it does affect the practical viability of a proposal.

Potential solutions are divided into the categories of current capabilities, legal measures, and exceptional access. The first option, in the category of current capabilities, is to do nothing. Some may conclude that the current state of affairs actually does represent an acceptable balance of interests. If technology and government agree on this approach, then the second crypto war can end much like the first. However, legislative action itself is a risk to be mitigated. If the technical community settles on this approach and government continues to reject it, the government could force its will and move encryption policy in a dangerous direction.

We could also decide to increase investment in current technologies and investigative techniques. As previously discussed, encryption is not the most significant barrier in law enforcement's use of digital evidence [120]. Even when encryption is involved, traditional sleuthing can often lead to access. Security expert Bruce Schneier and cyberlaw expert Orin Kerr have compiled a list of "encryption workarounds" that do not rely on EA. These include finding the key, guessing the key, accessing plaintext while the device is in use, and finding another copy of the plaintext [21]. Though probabilistic and time-consuming in comparison to EA, these methods do not require new legal or technical capability. These methods are effective [64]; due to their conservative nature, they are also safe.

Compelled password disclosure is a potential solution that simply requires defendants to surrender passwords and PINs to their devices. Questions regarding the legality of this approach have been working their way through the courts [62] [63] because of the apparent conflict with the Fifth Amendment right against self-incrimination. Affordability is the strongest argument

in favor of compelled password disclosure. Schneier and Kerr point out several weaknesses with this approach: prosecution must overcome the aforementioned legal hurdles, the password-holder must be available to investigators, and the password-holder must elect to provide the password [21]. Failing to provide the password may result in being found in contempt of court, but this would often be preferable to conviction of the original crime.

Lawful hacking is the most prominent proposed alternative to EA [123] [124] [2] [21] [61]. Lawful hacking's support may be due in part to the fact that it is a technical approach that isn't EA itself. However, its effectiveness against criminals for whom EA would not work is its obvious benefit. This is because, while organized crime and terror groups would still use encryption tools to evade an EA scheme, their operational security would fail at some point, letting law enforcement or intelligence agencies into their networks and devices. This approach has already been used [3], most famously to bring down cartel kingpin El Chapo [125]. Because it is already used, choosing lawful hacking as the primary strategy would require officially sanctioning, formalizing, and funding lawful hacking programs.

Despite its strengths, lawful hacking is a sub-optimal compromise. Because it requires time and specialized skills, it is not useful for small departments and commonplace crimes. It would also alter the relationship between law enforcement and tech companies. Law enforcement agencies would be forced into competition with tech companies if they were incentivized to conceal the vulnerabilities they discover. Prominent proposals suggest mandating disclosure of discovered vulnerabilities to mitigate this issue [123] [124]. Theoretically, there are enough vulnerabilities that, even though these discovered vulnerabilities would be disclosed and patched, new ones could be found quickly enough to enable steady levels of access. Government could source these vulnerabilities from a combination of the public domain, the commercial exploit market, and a central "Vulnerability Lab" [123].

The availability and cost of exploits fluctuates. For example, in January 2019, an Apple iOS jailbreak bug was valued at $2 million on the exploit market [126]. In contrast, a 2020 report revealed that cracking mobile devices cost law enforcement a mere $2000 per unit [118]. As the

exploit arms race continues, exploitability will be inconsistent. If law enforcement relies on lawful hacking as its strategy, it would face periods where it struggles for access, and would need to develop costly exploits in the lab. Mandatory vulnerability disclosure is necessary to avoid competition between law enforcement and tech companies. However, based on the FBI's historical abuses of power [34] and Congress's reluctance to fund initiatives it has passed [4] and failure to provide strong oversight [114], it seems unlikely that government would readily forfeit expensive vulnerabilities.

The final proposal is EA itself. EA would provide a standardized method for law enforcement to reliably access plaintext. It could compliment lawful hacking by eliminating the incentive to conceal vulnerabilities because hacking would be unnecessary for EA-compliant systems. When used together, EA would combat common crime and lawful hacking would combat organized crime and terror groups. EA's impact on civil liberties and mass surveillance would depend on its implementation. Any proposal would be costly to deploy and would threaten U.S. product competitiveness due to perceived insecurity. Increased security risk is EA's largest weakness. Any proposal must overcome significant challenges to minimize risk. The next map analyzes this more closely.

5.5 Zooming in on EA

Figure 5.6 maps the arguments surrounding several classes of EA. Weak cryptography, trusted-party key escrow, and distributed key escrow apply to both DAR and DIM. Device key escrow applies only to DAR, and cryptographic puzzles and ghost users apply only to DIM.

The first type of EA is simply the use of weak cryptographic ciphers or short encryption keys. This was the approach taken before the first crypto war, when strong cryptography was not readily available and was subjected to export controls. No party seriously supports this approach today, as far too many attackers would have the capability to abuse it.

Trusted-party key escrow relies on an entity or a small group of entities to store a key or key recovery information. There were a wide variety of trusted-party key escrow implementations

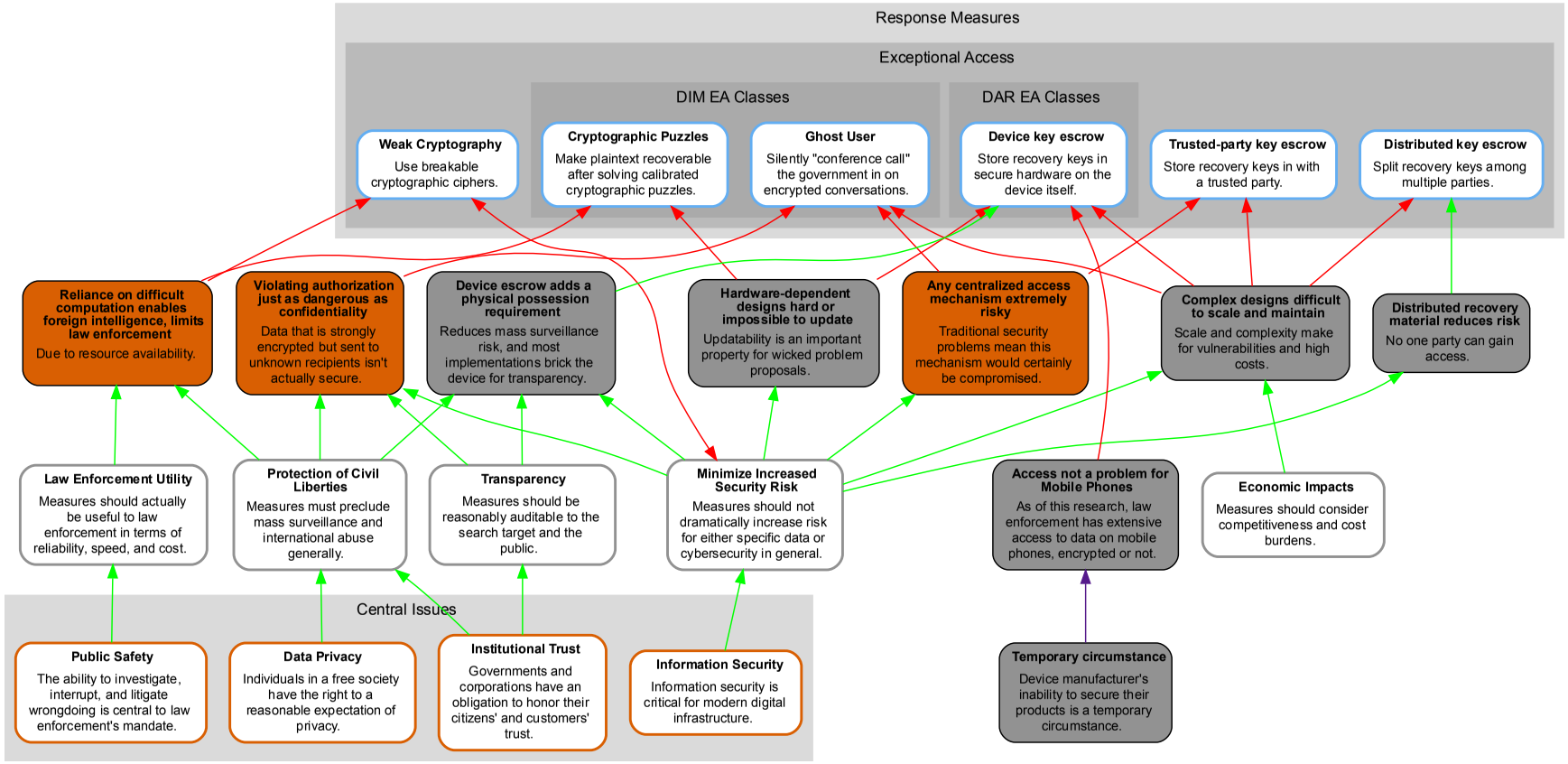

FIGURE 5.6 Classes of EA

created during the first crypto war [52]. This type of EA has a crushing weakness: it centralizes extremely sensitive information, which heightens the risk of a disastrous data breach. Some argue software companies are capable of protecting such sensitive data, citing their current practice of storing code-signing keys in Hardware Security Modules (HSMs) [57]. However, such keys are rarely used in comparison to EA keys, which would be updated and accessed frequently. Additionally, although code-signing keys are rarely used and are protected in HSMs, they still leak [127]. Once the escrowed keys leak, every device or message encrypted with them would be at risk. This is an example of the argument map's sometimes imbalanced portrayal of an argument's strength—in this case, the map underrepresents the effectiveness of the security-based argument against centralized access mechanisms.

Distributed key escrow differs from trusted-party in that it takes strong steps to remove centralized trust. This is achieved by using distributed systems to make key extraction difficult and publicly observable [54] [55]. One advantage of distribution over centralization is that it is more likely to fail safely. System failure would more likely result in *no one* to be able to recover plaintext instead of *anyone*. More research in this area is needed. Unfortunately, these systems would likely be costly to deploy and difficult to update due to their complexity.

One type of DIM EA uses strong cryptography but includes extra cryptographic "puzzle pieces" in message metadata. A surveiller could reconstruct the encryption key from the puzzle pieces, but only after expending considerable computational power [58] [59]. This approach precludes mass surveillance, but it also enables arbitrary surveillance by anyone with enough computing power. Using this type of DIM EA in common cases would be impractical due to its high cost. However, it would be less effective in high-profile cases due to the ability of sophisticated adversaries to employ EA workarounds. Additionally, puzzle difficulty would be calibrated based on the changing standards of computational capability. Since opponents can record data and decrypt it later when capabilities have changed, the data becomes steadily less secure over time.

Another DIM EA proposal involves adding authorities as a "ghost" participant in a conversa-

tion, analogous to a silent listener on a conference call. This was notably suggested by UK Government Communications Headquarters (GCHQ) officials Ian Levy and Crispin Robinson [128]. Their writeup is based on the same foundational principles as this thesis:

> In any discussion of cyber security, details matter.
>
> Unfortunately, it's the details that are missing from the discussion around lawful access to commodity end-to-end encrypted services and devices (often called the "going dark" problem). Without details, the problem is debated as a purely academic abstraction concerning security, liberty, and the role of government.
>
> There is a better way that doesn't involve, on one side, various governments, and on the other side lawyers, philosophers, and vendors' PR departments continuing to shout at each other. If we can get all parties to look at some actual detail, some practices and proposals—without asking anyone to compromise on things they fundamentally believe in—we might get somewhere. [128]

Although this proposal was raised with good intentions, it is nevertheless problematic. Proponents of the ghost user proposal consider the uncompromised use of strong encryption as the proposal's great strength. Although this is a good property, compromising a messaging app's authorization protocol is as dangerous as compromising its encryption [129]. Fundamentally, this proposal suffers from the same weakness as trusted-party key escrow—it introduces an authorization vulnerability in the messaging service provider's platform, resulting in dangerous centralized access capability [130]. It has a different form, but same nature as rejected key escrow proposals.

Finally, one type of DAR EA is device key escrow. In this scheme, key recovery material exists on the device itself. Most device key escrow proposals include physical possession requirements and make it clear when EA has been performed [56] [57]. Such features preclude mass surveillance and ensure transparency to the device user. This approach relies on secure hardware and a device unlock authorization process. The authorization process can be paired with other

EA strategies, such as storing keys with trusted-parties or distributed systems. This is where the weakness of the device escrow is revealed. First, secure hardware enclaves, though improving, are not totally reliable. Second, authorization to the hardware device is susceptible to the same attacks as traditional escrow EA.

Device key escrow's greatest weaknesses, however, are still signs of progress. While it does rely on a device's secure enclave, this is not a new risk. The same hardware device already manages device unlock and encryption functionality. Additional functionality increases the attack surface, but it does not add a completely new threat vector. While the authorization process is subject to the same problems as traditional key escrow after the device has been obtained, this is still an improvement over previous designs. Device key escrow requires the device to be obtained and cannot be used surreptitiously. Thus, advances in secure hardware design have meaningfully changed the EA risk profile.

In 2019, Carnegie Mellon assembled an ideologically diverse group of policy and security experts to engage in the kind of cross-disciplinary research. After describing every technical branch of the situation, their report identified the most promising branch: EA for domestic law enforcement (i.e., common cases instead of sophisticated adversaries) focusing on DAR in mobile phones using device key escrow requiring physical access [45]. This is because, as explained above, traditional investigation combined with lawful hacking is best suited for advanced opponents, while device key escrow represents actual progress towards low-risk EA for common crimes.

Device encryption, particularly in mobile phones, may actually pose the smallest impediment to investigation of any encryption technology. This fact undercuts the argument for device key escrow. The "Mass Extraction" report clearly describes the current state of affairs: device manufacturers are losing the exploit arms race, private companies are commodifying the lawful hacking approach for agencies large and small, and the lack of regulatory strategy is leading to pervasive data collection with little oversight [118]. This state of affairs reinforces the lessons of Chapter 3—inaction *is* action when facing wicked problems, and in this case, inaction has led to

an undesirable outcome. This situation does not negate the value of research into device-oriented EA. This is because the advantage hackers hold over device manufacturers is temporary; when law enforcement faces difficulty accessing devices again, this issue will immediately resurface. This is likely why law enforcement continues to push for EA despite present circumstances. Additionally, a formalized process may reduce government abuse, which threatens privacy and civil liberties more systematically than criminal abuse.

Despite device key escrow's tractability as a technical niche of EA, it is not ready for deployment. There are few proposals, the few that exist lack detail, and the matters of scaling and administration are unresolved. However, as incrementalism's Lindblom and even GCHQ's Levy and Robinson have pointed out, focusing on specific proposals may help to identify mutually agreeable solutions—or at least to refine the debate so that the next round of inquiry can be better informed.

The next chapter focuses on one specific device key escrow proposal. It defines a threat model and analyzes Stefan Savage's 2018 proposal, "Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion" [56].

CHAPTER 6

Threat Model

This chapter consists of a threat model and analysis of a specific device key escrow EA proposal, Stefan Savage's "Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion" [56]. The proposal is specific to data at rest for mobile devices. Due to the length of its title, this proposal will be referred to by its acronym, *LDAWMSR*. This chapter assumes that the proposal is accompanied by a legal framework regulating its application and use, though the legal framework is not the focus of this analysis.

6.1 Developing a Threat Model

"What are we building?" and "What can go wrong?" are the essential threat modeling questions. The process of answering these questions begins with setting goals, identifying threat actors, and declaring scope. The *LDAWMSR* proposal describes a threat model against which the proposal was designed. This threat model takes cues from the *LDAWMSR* model, but is intended to be more generally applicable for any DAR EA proposal.

6.1.1 Goals

The goals of an EA cryptosystem are taken from the five metrics used to judge EA alternatives and variations in Chapter 5. Each goal is listed according to priority, though no goal has absolute priority over the others.

- **Security**

  The system should minimize security risk relative to the current baseline. Risk is considered with respect to both individual devices and the entire class of devices.

- **Protection of civil liberties**

  The system should include measures to prevent mass surveillance and abuse by authoritarian regimes. This includes technologically enforcing the fundamental right to privacy outside the context of warranted search under the rule of law.

- **Transparency**

  The system should be auditable by the public to allow for verification that its power is being used responsibly. In the case of DAR, access should be apparent to the data owner.

- **Law enforcement utility**

  The system should be useful to law enforcement in terms of reliability, speed, and cost.

- **Economic impact**

  The system should consider global competitiveness of devices using the cryptosystem and the distribution of costs associated with its development and administration. Even though this is a security-oriented threat model, a system's design affects its economics, and its economics determines its ultimate feasibility.

6.1.2 Threat Actors

EA threat models include the full slate of traditional threat actors.

- **Criminals: ordinary, organized, cyber**

  Criminals threaten the EA system by using it to access plaintext without authority. Ordinary thieves may spy on targets or steal and resell phones. They will have physical access but only simple tools that use ordinary device interfaces. Organized criminals will have the same motives but considerably more advanced technical capabilities, including full control over all interfaces. Cyber criminals have a wide variety of of motivations and capabilities. They will target the backend systems that operate the EA system in order to abuse or sell whatever access capabilities they acquire.

- **Insider threat**

  Insider threats are attackers with roles inside the EA recovery process who seek to abuse the system for their own purposes. They could work in law enforcement, a device vendor, or a digital service provider. They may have the same motivations and skills of any other criminal category, but they have the advantage of privileged access at some stage in the process.

- **Foreign intelligence**

  Foreign intelligence agencies and advanced persistent threats (APTs) are constantly looking for ways to elevate their privilege and tamper with or steal information. They have world-class expertise and computing power, which they can apply to both individual devices and backend systems. (Here I am referring to *foreign* foreign intelligence agencies, as opposed to *domestic* foreign intelligence agencies such as the CIA or NSA in the U.S., which are assumed to operate within—though push the boundaries of—the legal framework.)

- **Authoritarian regimes**

  Governments that do not adhere to rule of law will try to compel administrators of an EA system to provide access upon demand. Legal coercion may or may not be combined with state-backed hacking capability.

Two non-traditional threats must be considered to make sense of an EA proposal in the face of the stated goals and such a formidable list of threat actors. Understanding these threats requires viewing security with a broader than usual perspective.

- **The platform abuser**

  The device user him or herself may actually be a threat in the larger safety context. Therefore, the end user's will is not the platform's top priority.

  All technologies have embedded values [111], and at the top of each value system is one top priority. Traditional device security threat models prioritize the will of end user. This leads to robust design decisions and honors the user's rights and autonomy.

  It is dangerous to stray from this rule, but many systems already do. Auto-updating software values the vendor's update policy over the user's preferences. Digital Rights Management software values corporations' data rights over the user's (sometimes to extremes [131]). Unencrypted e-mail software values the e-mail provider's ability to collect personal information over the user's privacy. Exceptional access systems value lawful investigation over the user's absolute privacy. Intentional subversion of the user's will violates a security practitioner's instincts, but it is a frequent reality.

  In the broader threat model, the platform abuser uses encryption to hide illicit activities. He or she is a threat to public safety.

- **Hawkish lawmakers**

  In the pursuit of security and privacy for society as a whole, aggressive lawmakers that have the power to *mandate* arbitrary data access present perhaps the largest threat of all. Crypto-anarchists will encrypt their data above the compromised layer regardless, but above-the-table organizations and most individuals who use default products will abide by U.S. law.

  Hawkish lawmakers threaten the security of a cryptosystem (whether it uses EA or not) because they may judge the system as too inhibitive to law enforcement. Therefore, they may outlaw its use and mandate something weaker in its place.

6.1.3 Out of Scope

The following considerations are beyond the scope of this threat model.

- **Encyption workarounds**

  Encryption workarounds, such as finding a copy of plaintext or guessing a password, are always a risk. Defending against such workarounds is not the role of the EA system itself.

- **EA workarounds**

  The user can evade EA mechanisms by encrypting data at a higher level in the tech stack, for example by encrypting files in software before saving them to disk. Additionally, investigators or attackers can often bypass current lockout mechanisms. This has already been discussed, and is not relevant when evaluating the EA system itself.

- **Supply chain attacks**

  It is necessary to protect device hardware and software supply chains in order to prevent surreptitious, trivially exploitable backdoors. For the purposes of this threat model, device hardware and software are assumed to be uncompromised, aside from the standard amount of bugs and side-channels.

- **Manipulation of internal hardware**

  Foreign intelligence agencies may have the capability to perform hyper-advanced hardware analysis and manipulation. Defending against these attacks is not the role of the EA system itself.

- **Breakdown in (or absence of) rule of law**

  This threat model assumes legitimacy of the legal process used to obtain the warrant. All forms of government search require oversight. Transparency via auditability, preferably ensured via technical mechanism, should be a goal for EA proposals. However, rule of law is an absolute prerequisite for which no EA mechanism can compensate.

6.2 Basic Data at Rest

Understanding the *LDAWMSR* proposal and comparing it to current mobile device encryption technology requires an understanding of current technology. Apple iPhones are among the most secure consumer mobile phones and serve as the point of reference for *LDAWMSR*. Because this analysis is limited to a specific proposal, it is also limited to this reference architecture. In Figure 6.1, a DFD depicts the iPhone's unlock and decryption process according to Apple's public documentation [132].

This DFD, and all that follow, presents the system at a specific level of abstraction. The system representation is simplified in the spirit of "all models are wrong, but some are useful." The DFDs exclude some details, but are accurate for the purposes of communication and threat elicitation.

As the diagram illustrates, several steps occur between the PIN being entered and the device being unlocked. The operating system forwards the PIN to the Secure Enclave Processor, which combines the PIN with the device-specific Hardware Unique ID (UID) to generate the Class key. The Class key is used to decrypt the Volume key, which is passed to the Encryption Module. The Encryption Module performs encryption and decryption at a hardware level between the operat-

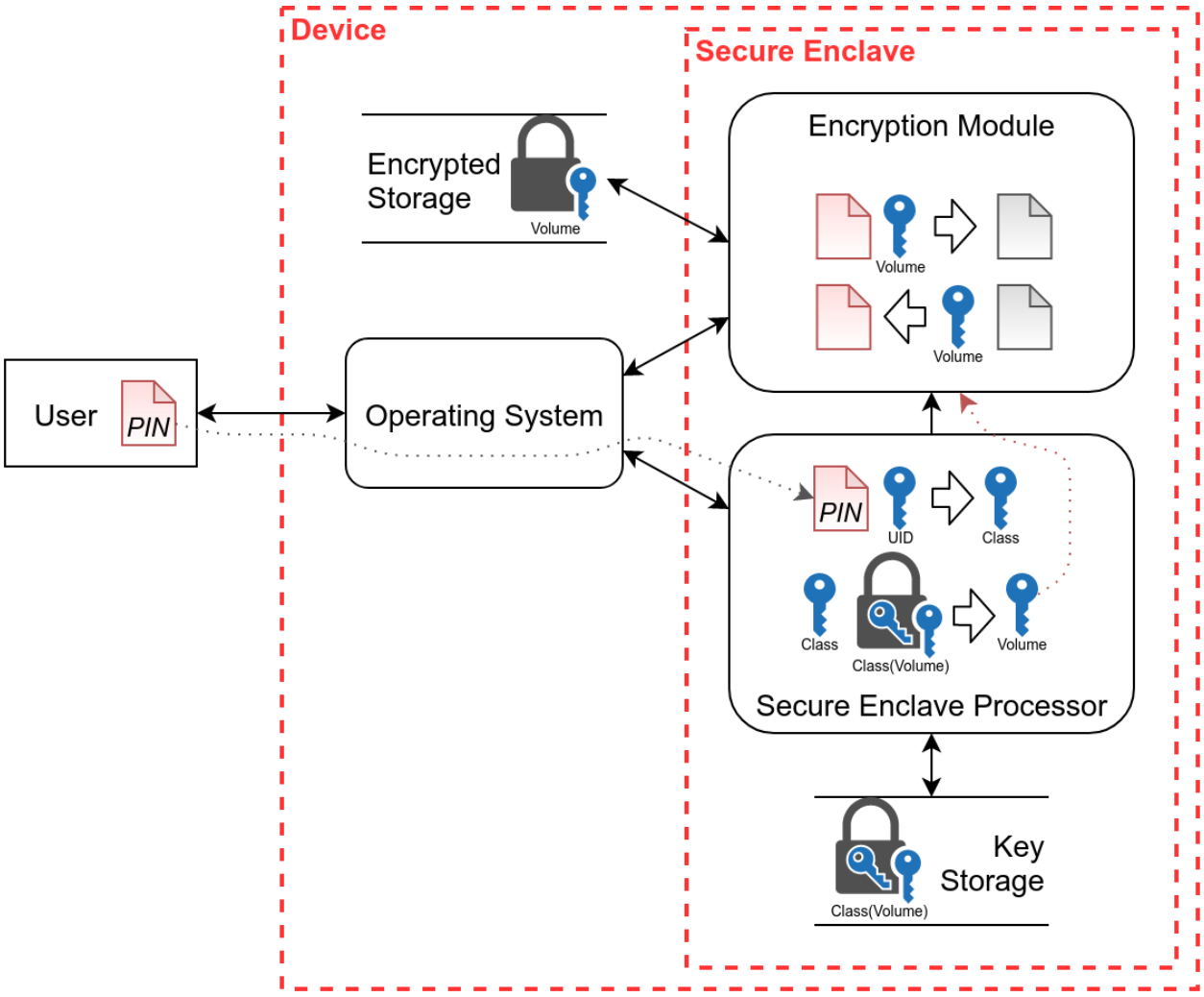

FIGURE 6.1 The basic encrypted mobile phone data flow diagram

ing system and the encrypted storage.

The UID is not depicted in key storage because it is burned into the secure processor silicon and cannot be read by software. The Volume key is encrypted by the Class key before it is stored. When a user updates his or her PIN, the encrypted Volume key in storage is replaced with the copy encrypted with the new Class key. Application processors do not handle any keys or secret information besides the PIN. Due to inline encryption in the Encryption Module, persistent storage does not handle plaintext data.

6.3 The *LDAWMSR* Proposal

LDAWMSR introduces device key escrow, an unexposed hardware interface that mediates EA requests, and a vendor-mediated authorization process. To achieve its goals, the proposal relies on the concepts of self-escrow, time vaulting, authorization, and transparency. These concepts are summarized in Table 6.1.

TABLE 6.1 Central Concepts in the *LDAWMSR* Proposal

Concept	Implementation	Outcome
Self-escrow	The Class key is escrowed in encrypted form in the device's Secure Enclave (or equivalent) using a write-only component; i.e., software can update the key, but only an unexposed hardware interface can read it.	Since the Class key itself is being stored instead of the encryption scheme being changed, there is no change to the security of the underlying cryptographic protocols. Physical possession and partial disassembly is required, which introduces practical barriers to mass surveillance.
Time vaulting	The hardware interface responds to requests only after proof of sustained possession for a "lockup period (e.g., 72 hours)."	The waiting period precludes "sneak and peak" attacks and further reduces the utility for mass surveillance.
Authorization	After the lockup period, the requestor must provide evidence of authorization. This comes from a shared secret between the device and the manufacturer which can be obtained via legal process.	Physical possession is now not enough; law enforcement (or attackers) must provide this secret information to the device to unlock it.
Transparency	In addition to the device disassembly, the escrow agent modifies the device (e.g., burns a fuse) when it has been unlocked. The device firmware detects this modification.	The device user has evidence that the device has been unlocked, preventing covert usage.

Device key escrow is considered the most promising technical EA direction because of the unique capabilities that secure hardware offers—namely, physical possession requirements and strong transparency. The physical possession requirement mitigates the risk of mass surveillance. As Savage adds, it also "provides a more intuitive compatibility with common under-standings of the government's reasonable law enforcement powers (e.g., the ability to seize physical property under court order) than more information-centric approaches, which may appear covert by com-

parison" [56]. Transparency is also rooted in the physicality of the approach, wherein the device cannot be unlocked without making irreversible and detectable changes, reducing the risk of both mass surveillance and common criminal abuse.

One clear weakness in the design is its reliance on the secret used in the authorization protocol shared between the device and the manufacturer. Although the key is stored on the device, anyone could access the key if they know the shared secret. This is similar to trusted-party key escrow. The vendor is the trusted party, and they store the authorization key rather than the encryption key itself. Due to this similarity, the problem of centralized risk is not fully addressed. This is discussed further in Section 6.4.

LDAWMSR's full data flow is illustrated in Figure 6.2. The proposal offers a few variations of the self-escrow and authorization protocols. This figure uses the asymmetric key pair approach for Class key encryption in the Secure Enclave, which creates strict hardware requirements. However, Savage offers a symmetric key variant that achieves the same purposes. The asymmetric key variant was chosen for analysis because it is semantically simpler.

When law enforcement needs access to a device, it first obtains a warrant to conduct the search. The warrant uniquely identifies the suspect's mobile device. Law enforcement obtains the device, disassembles it to reveal the unexposed EA hardware interface, and begins the time-vaulted access request. After the lockout period is completed, the device offers its Device ID only. The law enforcement agency's digital forensics department digitally signs the Device ID and sends it to the device vendor, alongside the warrant and accompanying proof of legal authorization. The vendor's access compliance department audits the legal documents and submits the digitally signed Device ID to a secure computing environment such as a HSM. The secure environment authenticates the digital signature, looks up the device's private Device Seal Key and authorization token, and encrypts them with the law enforcement agency's public key. These encrypted artifacts are returned to the agency, which decrypts and submits them to the device through the dedicated interface. First, the authorization token is hashed and compared to the stored hash. If the hash matches, the device accepts and uses the private Device Seal Key to de-

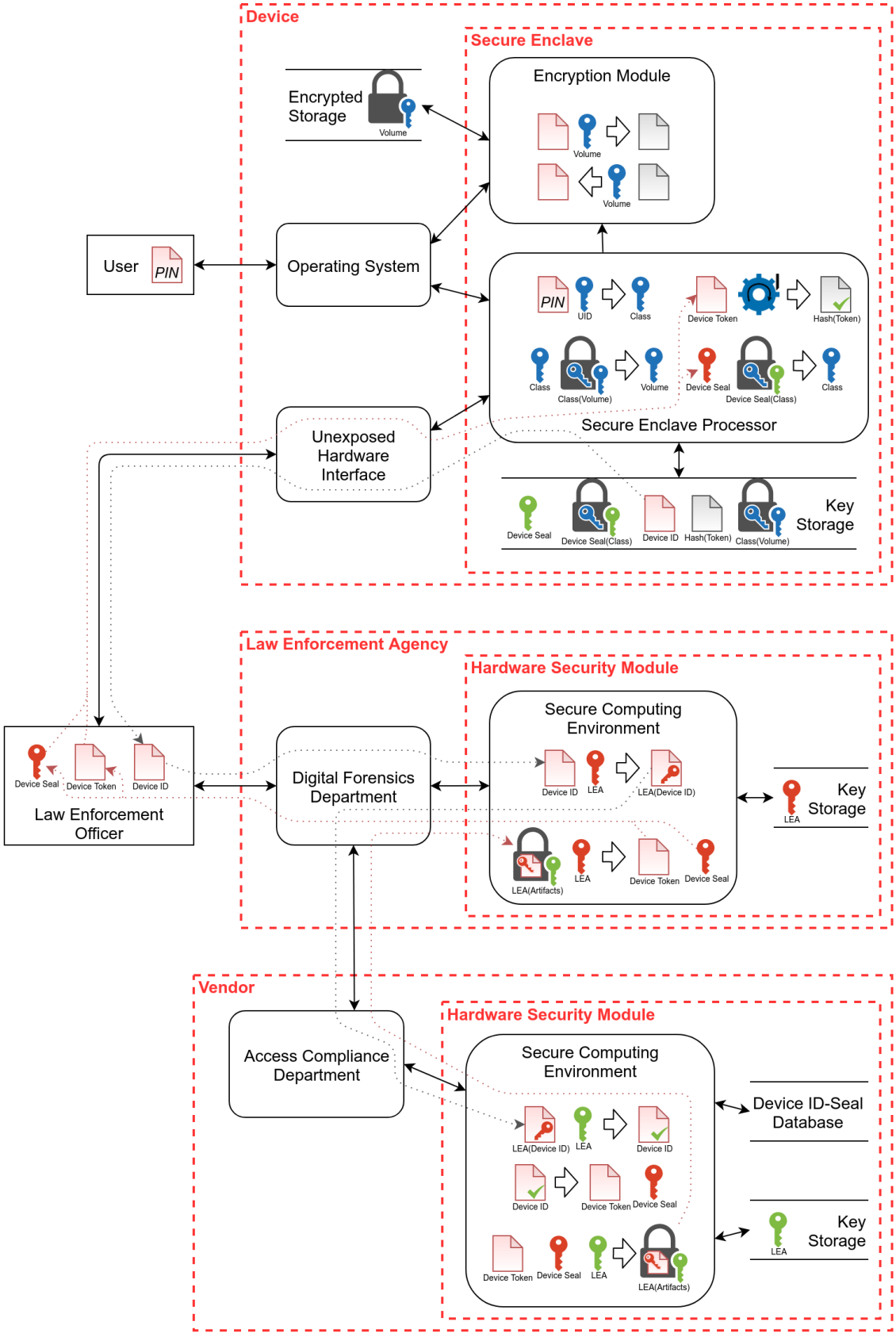

FIGURE 6.2 The LDAWMSR data flow diagram

crypt the Class key, which was escrowed after being encrypted but the public Device Seal Key. Once the Class key is decrypted, the escrow agent burns a fuse, and the device is unlocked for forensic investigation.

This above process is a summary of the system in the *LDAWMSR* proposal. However, complete proposals must account for the entire information lifecycle. In order to establish such a system, vendors and law enforcement must build mechanisms to populate and update the device and HSM key stores and databases. Figure 6.3 depicts a DFD for these scenarios.

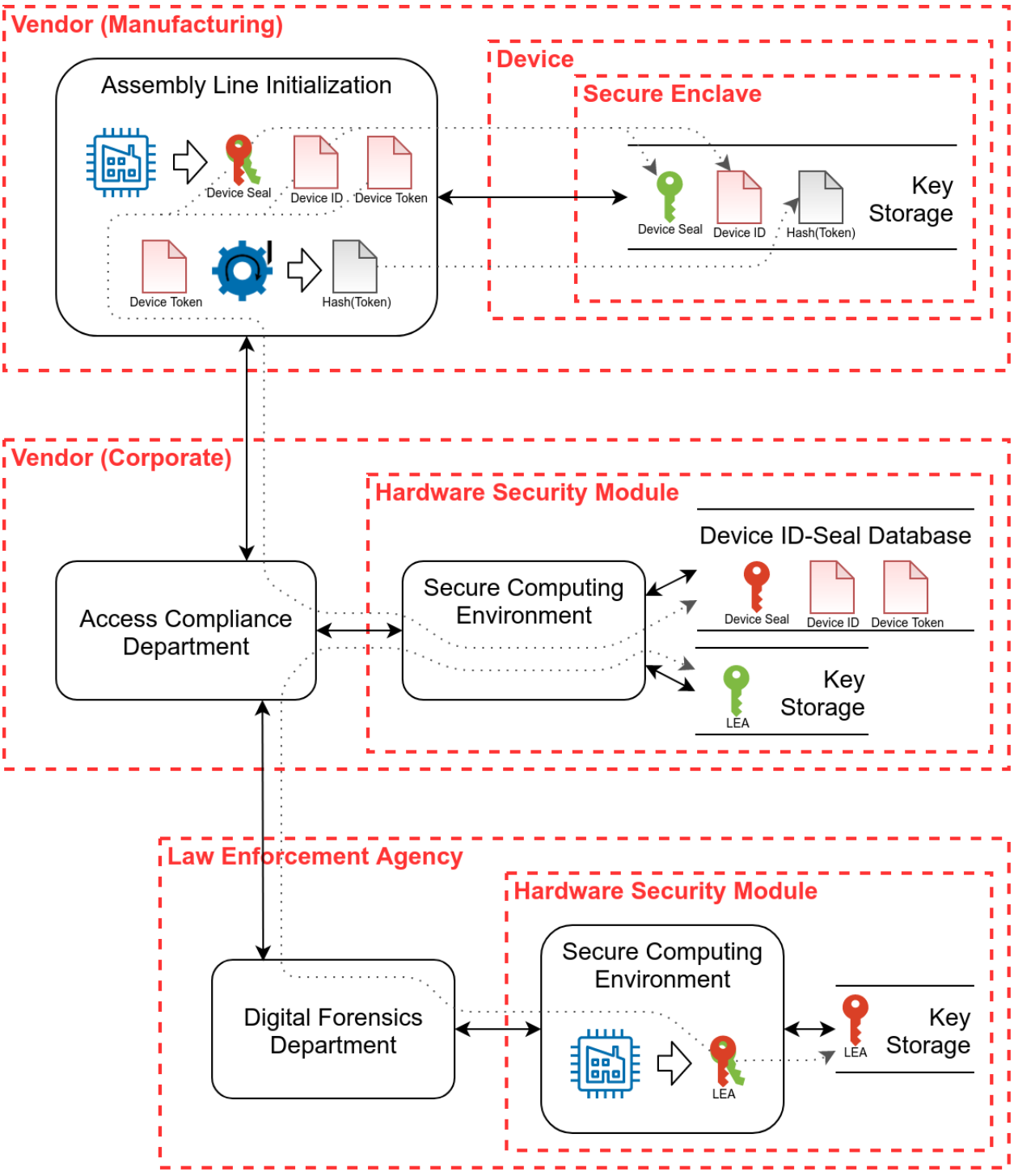

FIGURE 6.3 The LDAWMSR maintenance data flow diagram

6.4 Discussion of Threats

The next step in threat modeling is to elicit threats based on the system's goals, threat actors, scope, and design. Recall from Section 2.1 that security can be expressed in terms of authentication, integrity, non-repudiation, confidentiality, availability, and authorization. Threats are often expressed as the opposite of these properties: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege [13]. This section analyzes *LDAWMSR* according to these categories. Threats that could fall into multiple categories, such as tampering for the effect of repudiation, are listed only once.

To save space, the tables use shorthand for law enforcement (LE), law enforcement officer (LEO), law enforcement agency (LEA), Hardware Security Module (HSM), Device ID (DID), Device Seal Key (DSK), serial number (S/N), and denial of service (DOS).

6.4.1 Spoofing

Spoofing threats are listed in Table 6.2. Notably, *S2* is Eran Tromer's attack [133] on computer scientist Ray Ozzie's related DAR EA protocol called CLEAR [57]. Savage acknowledges the influence that CLEAR had on *LDAWMSR*, and specifically included a note that this proposal is technically vulnerable to the same threat. This threat is not particularly severe, as the difficulty of such an attack is so high that it is unlikely to be attempted. Even so, the mitigations listed here would also help.

TABLE 6.2 Spoofing Threats

ID	Spoof	Effect	Mitigation
S1	Device is spoofed to LE via plant	Attackers plant a device to get LE to unlock it for them.	Require the device to be in the forensics department itself the entire time it is unlocked.

TABLE 6.2 Spoofing Threats (continued)

ID	Spoof	Effect	Mitigation
S2	Device is spoofed to LE via forged DID	Attackers rig a device to report a different DID and record the entered unlock artifacts, allowing them into a target device.	Add a hardware integrity check or alternatively unlock the device in a Faraday cage (to prevent telemetry), extract its data, and destroy it (to prevent recovering stored data).
S3	LEO is spoofed to LEA	Attackers pose as a LEO while the LEA relays back unlock artifacts.	Require the device to be in the forensics department itself the entire time it is unlocked.
S4	LEA is spoofed to vendor during key exchange	Attackers pose as an LEA in order to spoof future access requests.	Vendor key exchange process involves thorough in-person verification. Assume only a handful of digital forensics laboratories nationwide are authorized to participate.
S5	LEA is spoofed to vendor during access request	Attackers pose as a LEA and submit an access request. Requires forged legal documents and a stolen LEA private key (unless attacker is an insider or has executed a spoofed key exchange).	Vendor independently verifies all legal documents. Vendor supports a key revocation and update process that involves the same level of in-person verification. Assume only a handful of digital forensics laboratories nationwide are authorized to participate.
S6	Manufacturer is spoofed to vendor	Attackers pose as the manufacturer to inject malicious data into the DID-DSK database. Must be combined with other attacks to be of use.	Vendor authenticates data transfers between manufacturing and corporate (does not address a compromised manufacturer network or an inside threat).

6.4.2 Tampering

Tampering threats are listed in Table 6.3. Note that execution of *S2* above relies on a tampering attack such as *T1*.

TABLE 6.3 Tampering Threats

ID	Tamper	Effect	Mitigation
T1	Platform abuser corrupts DSK, DID, or token	LE attempts at perform EA will fail due to corrupt data. Requires compromise of the Secure Enclave or advanced hardware manipulation tools.	Since these values are known at manufacturing time and never change, they can be made read-only. (The symmetric key variant of *LDAWMSR* requires updating the symmetric equivalent of the public DSK, and is therefore more vulnerable to this threat.)
T2	Platform abuser destroys the EA hardware interface	LE attempts to perform EA will fail due to damaged hardware.	Manufacture the device to require destructive disassembly to access the interface. This increases the cost associated with deploying and using the system.
T3	LE insider tampers with DID before digital signature	LEA receives an unauthorized device's unlock artifacts. Can be combined with other attacks to compromise a device.	Randomize DIDs to make them unguessable, meaning a target device must be in possession in order for the attacker to know what DID to use. Input to the vendor's HSM could also include data from the legal documents, such as device S/N; the HSM would append the S/N to the DID and hash the result, verifying a match with the same stored hash before returning the unlock artifacts.
T4	Attacker tampers with hardware transparency mechanism	The device user is unaware that the device was unlocked. Highly implementation dependent, but certainly requires advanced hardware manipulation tools.	Manufacture the device to require destructive disassembly to access the interface.

6.4.3 Repudiation

Repudiation threats are listed in Table 6.4.

TABLE 6.4 Repudiation Threats

ID	Repudiation	Effect	Mitigation
R1	Attacker or authoritarian government repudiates unlock attempt	The user is unaware that someone tried to access their device.	Manufacture the device to require destructive disassembly to access the interface, or use the same hardware transparency mechanism to mark mere access attempts as well.
R2	Authoritarian government repudiates demanding vendor assistance	Governments not respecting the legal framework governing the system can bully the vendor and try to force access while maintaining deniability.	This is close to being an out of scope threat under the "rule of law" exception. However, one could design the system to require requests and responses to be recorded on a public ledger. This creates several new difficulties.
R3	LEA repudiates having unlocked a device	The device is undeniably unlocked, but the LEA claims it was not them, allowing possible violations of civil liberties and harming transparency.	At a high level, the system should require a long paper trail before access can be granted. At a low level, the escrow agent could require and store some identifying information before unlocking, such as the LEA's public key digitally signed by the vendor, which provides non-repudiation assuming independent access to the device. See also the mitigation in *R2*.
R4	Vendor repudiates having responded to an access request	The device is undeniably unlocked, but the vendor claims they did not provide the unlock artifacts, allowing the vendor to cover up leaks or distasteful policy decisions by suggesting the device was instead hacked. Harms transparency.	Assuming independent access to the device, the hardware transparency mechanism should confirm whether the EA process was used, and the same identifying information used in *R3* would implicate the vendor. See also the mitigation in *R2*.

6.4.4 Information Disclosure

Information disclosure threats are listed in Table 6.5. In addition to the threats listed, any attack aimed at gaining unauthorized access to a device is an information disclosure threat. Most spoofing attacks aim to disclose information intended for another party.

TABLE 6.5 Information Disclosure Threats

ID	Information Disclosed	Effect	Mitigation
I1	Attacker discloses the DSK, DID, the encrypted class key, or hashed token	By design, none of the information stored on the phone is sensitive. The most consequential information that could be stolen is the DID, which could be paired with other attacks. Disclosing the DID requires either disassembly and time vaulting or advanced hardware inspection tooling.	Sensitivity of this data has already been mitigated as much as possible.
I2	Attacker intercepts unlock artifacts between LEA HSM and device	The attacker is able to unlock the target device alone. Must be combined with a spoofed DID to be of use to other devices (see *S2*). The attacker could record the values to replay them after the phone has been returned.	See *S2*. If choosing not to destroy the device, to prevent replay attacks, a new token could be generated and stored in the vendor HSM, with the new hash installed during the unlock process.
I3	Attacker steals the LEA private key	The attacker is now able to spoof the LEA and decrypt returned unlock artifacts. Without the devices (which are already in LE possession), the artifacts are not useful. See *S4* and *S5* for LEA spoofing attacks.	The key is stored in an HSM, which has extensive security measures. See *S5* for a revocation and update mitigation.
I4	Attacker steals the DID-DSK database	This is the big prize, the largest source of centralized risk. With the database, attackers could directly compromise any mobile device using this system in their possession, after disassembly, and after the time vault. They may also try to sell access to the data.	*R3* defines a mitigation that requires use of a vendor private key to create a digital signature as part of the authentication process. If used, that key would have to be compromised as well for the database to be of use. However, if the database is compromised, that key probably is too. Savage argues that HSMs, though imperfect, actually do provide very strong assurance. Responses could be rate-limited, and leaking an entire database once it's in the HSM could not go unnoticed. Getting the data in may be harder—see *I5*.

TABLE 6.5 Information Disclosure Threats (continued)

ID	Information Disclosed	Effect	Mitigation
I5	Attacker steals device unlock artifacts between manufacturing and vendor HSM	Intercepting the unlock artifacts at the source achieves the same effect as *I4*, only the data set is not complete. Instead of granting the ability to unlock any device, including a specific target, this is suited for getting access down the line or for sale.	The unlock artifacts generation process must be treated as sensitively as the HSM itself. The artifacts should be encrypted immediately and periodically transported to the corporate HSM on physical media. This threat is difficult to definitively mitigate.
I6	Attacker steals device plaintext from LEA after unlock process	Assuming the attacker doesn't care that the LEA gets access to plaintext, they could "help" the LE investigation in order to access the data later either when it comes out as public evidence or through compromising the LEA itself. This may be useful to authoritarian regimes, foreign intelligence, and organized crime.	LEAs must have strong information security of their own. Disclosure of evidence is a natural side effect of prosecution, so LEAs must practice discretion in choosing which devices to unlock in case mere information discovery poses a great risk in itself.

6.4.5 Denial of Service

Denial of service (DOS) threats are listed in Table 6.6. In addition to the threats listed, *S4* can be used for DOS by surreptitiously invalidating a LEA's identity key, and *T1* and *T2* are tampering attacks designed to deny LEAs from using the EA mechanism.

TABLE 6.6 Denial of Service Threats

ID	Service Denied	Effect	Mitigation
D1	Unlock artifacts recovery	*S6* could be used to inject corrupt data to the DID-DSK database, potentially overwriting actual unlock artifact data.	Verify integrity of new data before entering it into the database, and disallow overwriting entirely.
D2	Unlock artifacts recovery	Determined adversaries could physically destroy the medium storing the DID-DSK database.	The HSM should be in a physically secure and guarded facility, and the storage medium should be stable and persistent.

6.4.6 Elevation of Privilege

Elevation of privilege are listed in Table 6.7. Spoofing to usurp a entity's privilege or using any attack to unlock a device without authorization can be seen as elevation of privilege.

TABLE 6.7 Elevation of Privilege Threats

ID	Privilege Gained	Effect	Mitigation
E1	Foreign intelligence or organized criminals recruit an insider	The primary attacker gains inside access through coercion or bribery, making any other attack easier.	Limit the employees, accounts, and computers involved in any element of the system. Perform background checks on each employee and maintain detailed logs.
E2	Unexposed hardware interface allows access to Secure Enclave	The attacker gains access to Secure Enclave operations and data, undermining the device and achieving unlock without following the EA protocol.	The time vaulting protocol and all communication over the interface must be thoroughly tested, and if possible, formally proven to be logically sound. Analysis must include side channel attacks to affect the time vaulting or leak internal data.

TABLE 6.7 Elevation of Privilege Threats (continued)

ID	Privilege Gained	Effect	Mitigation
E3	An HSM vulnerability allows access to protected data	This is a technical route to achieving *I4*, disclosure of the DID-DSK database.	The HSM should be on an air-gapped network disconnected to the internet, physically guarded, and regularly patched. There is no defense against an unknown vulnerability, so security ultimately comes down to incident detection and response.

6.5 Risk Analysis

The amount of risk *LDAWMSR* introduces depends on the number of suggested mitigations that are implemented. Some possible attacks introduce inherently little risk due to their difficult nature and low pay off. Others introduce greater risk but can be reasonably addressed. Some threats specifically target transparency, and therefore are difficult to address without trust. Finally, there are some risks that cannot be safely mitigated. Each of these classes of threats are discussed in turn.

S6, *T1*, *T3*, *I1*, *I3*, *I6*, *D1*, *D2*, and *E1 E2* are each low-risk. They either are preventable, unuseful, or already present in the baseline depicted in Section 6.2. Although these threats are not fatal flaws to a design, it is important for a designer to consider and mitigate the risk they pose. Unless they appear in combination with other threats, they do not deserve more discussion.

S1, *S2*, *S3*, *S4*, *S5*, *T2*, *T4*, *R1*, and *I2* are all higher-risk threats to the security, trustworthiness, and effectiveness of the proposal. However, they can be mitigated through a set of related requirements: require destructive disassembly of the device to access the EA hardware interface, require the device to be physically present on LEA premises the entire duration it is unlocked, and grant only a handful of LE facilities the lawful right to use the EA mechanism. Requiring destructive disassembly entirely precludes certain attacks. Requiring the device to be on LEA premises prevents attackers from manipulating LE into achieving the attackers' ends. Limiting

the number of LE facilities that can participate in the EA process prevents LE impersonation attacks. Together, these mitigations make the proposal more resistant to attack.

R2, *R3*, and *R4* are repudiation attacks that belie the system's potential for abuse. The system relies on legal processes and cooperation of several parties. Even in the U.S., the legal process may involve secret courts, secret investigations, and secrecy orders on the vendor [34]. Under these conditions, transparency is difficult to achieve. The destructive disassembly requirement enables transparency at a device level. Auditable logs of device access *requests and responses* would enable transparency at a system level. *LDAWMSR* does not create such a log, though other DAR EA proposals do [54] [55] [134]. Unfortunately, building this feature into a proposal makes it potentially vulnerable the hawkish lawmaker, who may consider too much transparency to be an anti-feature.

Finally, there are the threats of *I4*, *I5*, and *E3*, which each represent the disclosure of unlock artifact data (the DID-DSK database). These threats create a large amount of risk that cannot be safely mitigated. Storing so much sensitive data in a central database creates a high-value target for foreign intelligence and cyber criminals. The vendor needs to protect this database from the most advanced attackers in the world while also regularly updating and accessing it. HSMs and robust security policies would make that a difficult task. However, the data will almost certainly leak eventually. The effects of such an event would depend on who stole the unlock artifacts. Criminals would use the data for personal and financial gain; foreign intelligence and authoritarian regimes would use it to spy on their enemies. In the worst-case scenario, anyone with specialized tools and disregard for the law could get into any compliant device after disassembling it and waiting through the time vault.

It is important to give *LDAWMSR* (and similar DAR EA proposals) its due. The worst case scenario still precludes mass surveillance and includes non-repudiation that access occurred. This is a significant gain for EA proposals in terms of transparency and protection of civil liberties.

6.6 Achievement of Goals

This chapter began with a list of goals by which DAR EA proposals can be measured, including security, protection of civil liberties, transparency, law enforcement utility, and economic impact. In this section *LDAWMSR* is measured against each of these goals.

Security. Security has already been discussed at length in this chapter. *LDAWMSR* introduces significant risk in the DID-DSK database itself, but performs well in many other respects, especially if the recommended mitigations are implemented. When the unlock artifacts are disclosed, the system becomes simple to attack. However, even in these conditions, attackers are limited to devices in their physical possession and cannot hide access from their victims.

Protection of civil liberties. This goal was defined as defending against mass surveillance and abuse by authoritarian regimes. *LDAWMSR* successfully protects against mass surveillance due to the physical possession and destructive disassembly requirements. It is not as effective against authoritarian regimes, which would put intense and possibly coercive legal pressure on vendors to unlock devices. In the case of an unlock artifacts leak, regimes could broadly abuse the system. This technology would be unwelcome to those living in countries that do not respect rule of law.

Transparency. *LDAWMSR* provides transparency to the device user, but does not provide transparency to the public. As discussed in the previous section, the destructive disassembly requirement would result in transparency at the device level. However, access to a device can only be confirmed if the device is available. Neither the user nor the public can detect if a device has been unlocked under secretive conditions, whether lawfully or criminally. This creates potential for government abuse.

Law enforcement utility. *LDAWMSR* includes a few tradeoffs between security and law enforcement utility. The requirements to have physical possession of the device, to wait through the time vault, and to limit the number of authorized law enforcement laboratories all create barriers to usability. The physical possession requirement is too important for security to be compromised

for utility. Additionally, search and seizure law is already designed for physical evidence; maintaining the possession requirement makes the system operate within well-understood norms. The time vault prevents against time-sensitive attacks, though destructive disassembly (not part of the original proposal) may be enough to cover these cases. The time vault period could be decreased without significant impact. Limiting the number of laboratories that can use the system reduces the risk of spoofing attacks; local law enforcement would have to cooperate with one of these special laboratories, such as a regional FBI office, to unlock a device. In the end, law enforcement still has a reliable way to get into lawfully seized devices. *LDAWMSR* does its part, but the government must fund the FBI operation and cultivate cooperation between local and federal agencies.

Economic impact. Expenses to the vendor fall into three categories—the costs of implementing the design, running the system, and absorbing lost business. Even if a proposal like *LDAWMSR* was refined enough to be implemented, the vendor would need to update hardware designs and create the software systems to get it started. Once in use, the vendor would face considerable costs in running it securely due to the difficulty of safely accessing and updating the unlock artifacts. Finally, the vendor would certainly lose privacy-conscious customers to small businesses, foreign competitors, or resellers offering pre-EA devices. The scale of these costs relative to device manufacturer's large size is unclear. Costs to the government include the FBI laboratory cost and the cost of law enforcement resources and training. CALEA includes provisions for government reimbursement of vendor compliance costs, and a similar provision could be applied to DAR EA regulation [70].

CHAPTER 7

Paths Forward

The interests of security, safety, privacy, and trust converge on the issue of encryption and exceptional access, creating a wicked problem. The importance of information security is increasing as more data, business, and infrastructure goes online. The technical community struggles with security. Even for the most well-equipped organizations, thwarting the average attacker is difficult, and the best attacker, impossible. Cryptography plays a fundamental role in security, yet it remains a controversial technology due to its simultaneous role in enabling unprecedented privacy.

First, proponents of exceptional access argue that encryption-enabled privacy as harmful effects on public safety. Despite a shortage of quantitative analyses showing its impact on crime, encryption certainly does allow evidence of wrongdoing to be hidden from service providers and law enforcement. This enables harmful activity to go unchecked and decreases public safety, which is a legitimate concern and the primary motivation for EA.

However, while encryption adds privacy, technological change as a whole is stripping it away. The ubiquity of modern computing has created terabytes of data on every individual; access laws, business models, and insecurity have exposed this data to huge audiences. This trend has enabled mass surveillance, inappropriate data mining, identity theft, and other threats. When encryption mitigates these threats, it increases public safety.

Finally, deciding how to respond to these issues—whether with inaction, EA, or some alternative—requires determining what institutions are worthy of trust. Potential solutions assign different levels of trust to law enforcement agencies, intelligence agencies, technology makers, individual users, and the public at large. Each of these groups have demonstrated untrustworthiness, but all paths forward require putting trust somewhere.

This complex mix of issues makes encryption policy a wicked problem. Even formulating the problem requires several iterations of research into history, arguments, and technology. Every formulation presupposes a solution, but the effectiveness of a solution cannot be accurately eval-

uated. Meanwhile, the underlying conditions constantly change due to external forces and policy actions (or lack thereof).

In this thesis, I propose a method to confront wicked problems based on a modified OODA Loop. The method emphasizes collaborative debate between diverse individuals, facilitated in part by argument maps and focused on specific proposals. The second half of the thesis applies this method by surveying the debate, mapping the arguments, and ultimately performing threat model analysis of a specific EA proposal for data at rest. I now turn to conclusions and paths forward for both the technical and policymaking communities.

7.1 Conclusions

Based on the arguments analyzed in Chapter 5, neither side of the EA debate addresses all of the root issues. However, given the wide gap between the requests of government officials and the maturity of EA technology, the anti-EA argument is currently stronger. Encryption does pose certain threats to public safety. Terrorists and criminals can and do use encryption to evade the law; in particular, this has allowed for shocking levels of child sexual abuse material (CSAM) to be peddled [4]. However, the argument that encryption is causing law enforcement failure is unsubstantiated at this time. For data in motion, poor coordination and training hamper law enforcement more than encryption [120]. For data at rest, commercial lawful hacking tools currently outdo mobile phone manufacturers, meaning law enforcement can get into almost any mobile device they acquire [118]. Additionally, strong encryption is a necessary tool in protecting security and privacy—two public goods that other technological developments often fail to provide.

Though the pro-EA argument does not justify an EA mandate, it can teach technologists some important lessons. First, holistic cryptosystem threat models must include two non-traditional threat actors, the malicious user and threatening lawmaker. Encryption lends power to its user, and this power can be abused. Technology makers must include abusive use in their threat modeling. Governments are inherently sensitive to changes in personal privacy; lawmakers therefore represent a unique threat because they can outlaw uses of encryption entirely if they deem them

too dangerous. The danger of an EA mandate must also be included in the cryptosystem threat model.

Second, EA history teaches that the current situation is temporary. This is true of all wicked problems, but especially for encryption policy due to rapidly evolving technology and a vulnerability arms race between device manufacturers and lawful hackers. Circumstances are sure to change, and the conclusion that EA is unjustified may change as well.

Further research into EA is warranted due to the additions to the threat model and the instability of present circumstances. Fortunately, developments in secure hardware mark real progress in the search for acceptably secure EA. Secure hardware technology is not perfect; on its own, it does not resolve the numerous challenges that full-fledged EA proposals must overcome. However, EA proposals leveraging secure hardware, such as device escrow for data at rest, represent progress. They offer transparency, protection from mass surveillance, and law enforcement utility while remaining somewhat secure.

The conclusions presented here do not settle the issue. However, when dealing with wicked problems, meaningful discussion can be considered progress even if it does not reach concrete resolution. Much of the work involved in confronting wicked problems is understanding the problem itself. The conclusions above do not bring closure, but clarity.

7.2 Paths Forward: Technology Makers

It is the responsibility of the technical community to accept and address the substantial role technology plays in current policy issues, such as encryption, automation, and misinformation. Government sometimes suggests that the tech world simply needs to try harder. Because these are not tame problems, the tech world is absolutely right that simply trying harder will not work—but that does not mean they cannot deal with them. The tech industry is optimized to address tame problems, but it must now turn its financial and intellectual capital towards strategies designed for wicked problems. In order to do so, the tech industry must involve people of diverse backgrounds and values in design and investment decisions. Designers must consider the ways

in which their products could be abused, and business models must be responsive to evolving conditions.

Addressing wicked problems reveals smaller subproblems, some tame and some also wicked (see Figure 3.5). In addition to making changes to tackle wicked problems directly, the technical community should also address the tame subproblems. Some suggestions for doing so are listed below.

- **Basic security research**

  EA is only worthwhile when basic security renders lawful hacking insufficient, which is not the case for current device encryption. This is a security ergonomics problem more than a technical problem—cryptographers are already capable of creating stronger device encryption, but users would rebel due to its adverse effects on usability. Solving the strong-yet-usable device encryption problem will make the most promising class of EA, device key escrow, relevant. Improving security in general will make any EA proposal more tenable.

- **Research technical transparency mechanisms**

  One of the largest non-technical risks of EA is its potential abuse by jurisdictions with poor rule of law. This is the reason transparency is a goal of the threat model. Device key escrow can achieve partial transparency through physical possession and disassembly requirements. Ideally, usage of EA mechanisms would be fully auditable to the public through inherent technical mechanisms. This can be improved for data at rest and must be improved for data in motion.

- **Research distributed trust mechanisms**

  Most EA proposals would still result in a concentrated center of risk, whether it would take the form of a database of keys or of a control center with the ability to add "ghost users" to conversations. As explained in Section 1.2, insecurity cannot be destroyed, it can only be moved around. Distributed trust mechanisms avoid assigning a large amount of trust to any single party. This contributes to both transparency and security.

Fortunately, this research is already happening to some degree, though more is necessary. Some EA proposals include built-in transparency and distributed trust mechanisms [53] [54] [55]. Like device key escrow, approaches such as these hold promise, but must be better understood before they could be implemented. Even while these problems remain unsolved, technologists must provide clear security advice and speak out against bad policy.

7.3 Paths Forward: Policymakers

Policymakers have not been silent on the issue of encryption and lawful access. The influence of the executive, legislative, and judicial branches ensures that the regulatory environment will evolve with changing federal policies, laws, and rulings. The judiciary will shape encryption policy through its rulings and by reevaluating Fourth Amendment jurisprudence in light of rapidly changing circumstances. Still, the primary actors capable of consciously taking part in strategic policymaking will be the executive and legislative branches.

Executive and legislative policymakers must strategically approach encryption policy as a wicked problem. Industry has failed to resolve the problem with analysis, and government has failed to resolve the problem with incrementalism. Incrementalism has safely avoided dangerous outcomes such as blanket EA mandates. However, it has also resulted in a research-stifling debate, the poor utilization of current capabilities, and the unregulated use of invasive lawful hacking tools. While policymakers and law enforcement agencies have made important contributions to the debate, they need to share data more openly. Just like the technical aspects, the policy as-

pects of the solutions must be responsive to evolving conditions.

Based on the analysis performed thus far, the following steps could be taken today.

- **Take the low-hanging fruit**

  Law enforcement is ill-equipped to access digital evidence with existing mechanisms [120]. Justice Department task forces for combatting child sexual abuse material are underfunded and understaffed [4]. Investment in existing programs will likely produce results without introducing risk.

- **Regulate current lawful hacking**

  Lawful hacking using commercial mobile device forensic tools has become a common practice; this invokes serious privacy and civil rights concerns [118]. Regardless of long-term encryption policy strategy, lawful hacking must be regulated. Michigan's 2020 constitutional amendment represents one positive development: it explicitly protects electronic data and communications from search without a warrant [135]. Protections like this can prevent abuse of current lawful hacking capability.

- **Fund research**

  Lawmakers request research into EA technology, but private companies lack financial incentive and universities lack interest due to the threatening climate. The federal government cannot compare building secure EA to going to the moon if it does not provide the same level of funding. In order to be welcomed by the academic community, such funding must be accompanied by a binding statute excluding the possibility of a premature EA mandate.

7.4 Decision and Action

The goal of this thesis is to establish encryption policy as a wicked problem, to analyze the debate, and to evaluate the security of current EA technology. I aim to advance the discussion

with a strategy to tackle wicked problems, additions to the cryptosystem threat model, and detailed analysis of a modern proposal. The strategy is based on the *Observe-Orient-Decide-Act* Loop. In those terms, this paper serves to *observe* and *orient*. Technologists, policymakers, and common people must *decide* and *act*. Confronting these issues may be difficult, but the future of security, safety, and privacy depends on finding an acceptable solution where no perfect solution exists.

Glossary

AECA Arms Export Control Act.

APT advanced persistent threat.

argument map A graphical representation of the logical structures and relationships between statements, premises, and conclusions, used to disentangle complex arguments used in wicked problems .

asymmetric cryptography A cipher scheme where encryption and decryption are performed with separate, paired keys, called the public key and the private key .

AWA All Writs Act.

CALEA Communications Assistance for Law Enforcement Act.

CESA Cyberspace Electronic Security Act.

CFAA Computer Fraud and Abuse Act.

CIA Central Intelligence Agency.

cipher A tool or algorithm to perform encryption, translating between plaintext and ciphertext .

ciphertext Encrypted data.

classical analytic method A policy making strategy that emphasizes rationalism and functions by setting goals, identifying problems, evaluating alternatives, implementing solutions, and analyzing outcomes in order to correct errors .

Clipper Chip A 1993 initiative by the Clinton administration to provide "the public with strong cryptographic tools without sacrificing the ability of law enforcement and intelligence agencies to access unencrypted versions of those communications" via hardware additions

to consumer electronics. The proposal faced opposition, and died in 1994 when security researcher Matt Blaze discovered flaws that allowed users to subvert the Clipper Chip mechanisms .

cryptography The study of techniques for communicating secretly in the presence of third parties .

CSAM child sexual abuse material.

DAR data at rest.

DE device encryption.

decryption The process of translating from ciphertext to plaintext.

DFD data flow diagram.

DID Device ID.

DIM data in motion.

disk encryption An application of ecnryption for DAR that involves encrypting the contents .

DOS denial of service.

DSK Device Seal Key.

E2EE end to end encryption.

EA exceptional access.

EARN IT Act Eliminating Abusive and Rampant Neglect of Interactive Technologies Act.

ECPA Electronic Communications Privacy Act.

ENCRYPT Act Ensuring National Constitutional Rights for Your Private Telecommunications Act.

encryption The process of translating from plaintext to ciphertext.

FBI Federal Bureau of Investigation.

FISA Foreign Intelligence Surveillance Act.

FISAAA FISA Amendments Act.

forward secrecy A property of DIM encryption protocols that ensures that a leaked private key or session key does not compromise any other private key or session key .

Four Horsemen Four reasons that governments and law enforcement agencies use to undercut public support for strong encryption. The four horsemen are terrorists, pedophiles (child pornographers), drug dealers (and traffickers), and money launderers (or kidnappers) .

GCHQ Government Communications Headquarters.

HSM Hardware Security Module.

IBIS issue-based information system.

incrementalism A policy making strategy that functions by taking successive steps based on the status quo and chosen through comparative analysis; also known as “muddling through” .

ITAR International Traffic in Arms Regulations.

key Secret information required to operate the cipher and perform encryption and decryption.

key escrow An approach to EA that relies on storing additional copies of the encryption key or storing information that can be used to derive additional additional copies .

LAED Act Lawful Access to Encrypted Data Act.

lawful hacking An approach to digital evidence and intelligence gathering that involves deliberate computer and network manipulation which is ordinarily illegal but has been cleared for law enforcement and intelligence purposes .

LDAWMSR A reference to computer scientist and security researcher Stefan Savage's device key escrow proposal, "Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion" [56] .

LE law enforcement.

LEA law enforcement agency.

LEO law enforcement officer.

mass surveillance Ubiquitous data collection and analysis by remote, centralized bodies .

muddling through See "incrementalism" .

NSA National Security Agency.

NSL National Security Letter.

OODA Loop *Observe-Orient-Decide-Act* Loop.

PGP Pretty Good Privacy.

PIN personal identification number.

plaintext Unencrypted data.

PRISM An NSA program unveiled by Edward Snowden involving the mass collection of internet communications data of non-U.S. persons and those communicating with them .

Pro-C0DE Act Promotion of Commerce On-Line in the Digital Era Act.

public key cryptography Another name for asymmetric encryption .

replay protection A property of DIM encryption protocols that ensures that messages cannot be replayed by an attacker without detection .

S/N serial number.

SAFE Act Security and Freedom Through Encryption Act.

symmetric cryptography A cipher scheme where encryption and decryption are performed with the same key .

the first crypto war The flurry of evolution and conflict in encryption policy during the 1990s, characterized by episodes around export controls, PGP, the Clipper Chip, and early key escrow proposals .

the Four Horsemen of the Infocalypse The long name for "The Four Horsemen".

the second crypto war The flurry of conflict in encryption policy during the late 2010s to present, characterized by angst from the Snowden revelations, the proliferation of strong encryption, and the Apple vs. FBI case .

UID Unique ID.

USA FREEDOM Act Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act.

USA PATRIOT Act Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.

wicked problem A problem lacking clear formulations, causes, resolutions, or metrics. Consistenly difficult to solve, and often social or political in nature .

Bibliography

[1] H. W. J. Rittel and M. M. Webber, "Dilemmas in a general theory of planning," *Policy Sciences*, vol. 4, no. 2, pp. 155–169, Jun. 1973. [Online]. Available: http://link.springer.com/10.1007/BF01405730

[2] A. Z. Rozenshtein, "Wicked Crypto," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3256858, Oct. 2018. [Online]. Available: https://papers.ssrn.com/abstract=3256858

[3] J. Cox, "How Police Secretly Took Over a Global Phone Network for Organized Crime," jul 2020. [Online]. Available: https://www.vice.com/en_au/article/3aza95/how-police-took-over-encrochat-hacked

[4] M. H. Keller and G. J. X. Dance, "The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?" *The New York Times*, Sep. 2019. [Online]. Available: https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html

[5] F. C. Ministerial, "Five country ministerial 2018," 2018. [Online]. Available: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018

[6] P. Patel, W. Barr, P. Dutton, A. Little, B. Blair, Japan, and India, "International Statement: End-To-End Encryption and Public Safety," Oct. 2020. [Online]. Available: https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

[7] J. B. Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" oct 2014. [Online]. Available: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

[8] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier,

M. A. Specter, and D. J. Weitzner, “Keys under doormats: mandating insecurity by requiring government access to all data and communications,” *Journal of Cybersecurity*, p. tyv009, Nov. 2015. [Online]. Available: https://academic.oup.com/cybersecurity/article-lookup/doi/10.1093/cybsec/tyv009

[9] Eighty-three civil society organizations and eminent individuals, “To ministers responsible for the five eyes security community,” Jun. 2017. [Online]. Available: https://www.efa.org.au/main/wp-content/uploads/2017/06/Coalition-Letter-to-5eyes-Govs.pdf

[10] D. Ruiz, “There is No Middle Ground on Encryption,” May 2018. [Online]. Available: https://www.eff.org/deeplinks/2018/05/there-no-middle-ground-encryption

[11] N. R. Council, *Trust in Cyberspace*, F. B. Schneider, Ed. Washington, D.C.: National Academies Press, Jan. 1999. [Online]. Available: https://www.nap.edu/catalog/6161/trust-in-cyberspace

[12] S. M. Bellovin, *Thinking security stopping next year’s hackers*. New York: Addison-Wesley, 2016, oCLC: 1047874327.

[13] A. Shostack, *Threat modeling: designing for security*. Indianapolis, IN: Wiley, 2014, oCLC: ocn855043351.

[14] R. S. Mueller, “U.S. v. Viktor Borisovich Netyksho, et al,” jul 2018. [Online]. Available: https://www.justice.gov/file/1080281/download

[15] A. Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *Wired*, aug 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[16] D. Goodin, “Ransomware forces 3 hospitals to turn away all but the most critical patients,” Oct. 2019. [Online]. Available: https://arstechnica.com/information-technology/2019/10/hamstrung-by-ransomware-10-hospitals-are-turning-away-some-patients/

[17] D. Luciano and G. Prichett, “Cryptology: From Caesar Ciphers to Public-key Cryptosystems,” *The College Mathematics Journal*, vol. 18, no. 1, pp. 2–17, Jan. 1987. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/07468342.1987.11973000

[18] D. Kahn, *The codebreakers: the story of secret writing*, 2nd ed. New York: Scribner, 1996.

[19] C. E. Shannon, “Communication Theory of Secrecy Systems*,” *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6769090

[20] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976. [Online]. Available: http://ieeexplore.ieee.org/document/1055638/

[21] O. S. Kerr and B. Schneier, “Encryption Workarounds,” Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2938033, Mar. 2017. [Online]. Available: https://papers.ssrn.com/abstract=2938033

[22] D. Kehl, “The Right to Strong Encryption Almost Became Law in the ’90s,” Jun. 2015. [Online]. Available: https://slate.com/technology/2015/06/safe-act-the-right-to-strong-encryption-almost-became-law-in-the-90s.html

[23] P. Zimmermann, “Phil Zimmermann’s Senate Testimony,” jun 1996. [Online]. Available: https://www.philzimmermann.com/EN/testimony/index.html

[24] W. H. Press Secretary, “White House Annoucement of the Clipper Initiative,” apr 1993. [Online]. Available: https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/clipper-announcement.html

[25] A. W. Thompson, D. Kehl, and K. Bankston, "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s," jun 2015. [Online]. Available: https://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/

[26] M. Blaze, "Protocol failure in the escrowed encryption standard," in *Proceedings of the 2nd ACM Conference on Computer and communications security - CCS '94*. Fairfax, Virginia, United States: ACM Press, aug 1994, pp. 59–67. [Online]. Available: http://portal.acm.org/citation.cfm?doid=191177.191193

[27] C. R. Burns, "S.1726 - 104th Congress (1995-1996): Promotion of Commerce On-Line in the Digital Era (Pro-C0DE) Act of 1996," Jul. 1996. [Online]. Available: https://www.congress.gov/bill/104th-congress/senate-bill/1726

[28] B. Goodlatte, "H.R.3011 - 104th Congress (1995-1996): Security and Freedom Through Encryption (SAFE) Act," Sep. 1996. [Online]. Available: https://www.congress.gov/bill/104th-congress/house-bill/3011

[29] W. Clinton, "Executive Order 13026—Administration of Export Controls on Encryption Products," nov 1996. [Online]. Available: https://www.presidency.ucsb.edu/documents/executive-order-13026-administration-export-controls-encryption-products

[30] P. Rodino, "H.R.7308 - 95th Congress (1977-1978): Foreign Intelligence Surveillance Act," Sep. 1978. [Online]. Available: https://www.congress.gov/bill/95th-congress/house-bill/7308

[31] M. C. Gizzi and R. C. Curtis, *The Fourth Amendment in flux: the Roberts court, crime control, and digital privacy*. Lawrence, Kansas: University Press of Kansas, 2016.

[32] W. Bloss, "Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects," *Surveillance & Society*, vol. 4, no. 3, Sep. 2007. [Online]. Available: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3448

[33] J. Sensenbrenner, "H.R.3162 - 107th Congress (2001-2002): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001," Oct. 2001. [Online]. Available: https://www.congress.gov/bill/107th-congress/house-bill/3162

[34] H. Shamsi and A. Abdo, "Privacy and Surveillance Post-9/11," *Human Rights*, vol. 38, p. 5, 2011. [Online]. Available: https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/human_rights_vol38_2011/human_rights_winter2011/privacy_and_surveillance_post_9-11/

[35] E. Tucker, "Watchdog finds new problems with FBI wiretap applications," Mar. 2020. [Online]. Available: https://apnews.com/7dad2d06850ce331b8953281371e8b61

[36] S. Landau, "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations," *IEEE Security & Privacy*, vol. 11, no. 4, pp. 54–63, Jul. 2013. [Online]. Available: http://ieeexplore.ieee.org/document/6573302/

[37] F. Tréguer, "US Technology Companies and State Surveillance in the Post-Snowden Context: Between Cooperation and Resistance," CERI, report, Dec. 2018. [Online]. Available: https://halshs.archives-ouvertes.fr/halshs-01865140

[38] M. Schulze, "Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016," *Media and Communication*, vol. 5, no. 1, p. 54, Mar. 2017. [Online]. Available: http://www.cogitatiopress.com/mediaandcommunication/article/view/805

[39] S. Stalla-Bourdillon, "Privacy Versus Security… Are We Done Yet?" in *Privacy vs. Security*. London: Springer London, 2014, pp. 1–90. [Online]. Available: http://link.springer.com/10.1007/978-1-4471-6530-9_1

[40] B. Schneier, "Attorney General Barr and Encryption - Schneier on Security." [Online]. Available: https://www.schneier.com/blog/archives/2019/08/attorney_genera.html

[41] J. Novet, “Apple vs. FBI: A timeline of the iPhone encryption case,” Feb. 2016. [Online]. Available: https://venturebeat.com/2016/02/19/apple-fbi-timeline/

[42] R. Burr and D. Feinstein, “Intelligence Committee Leaders Release Discussion Draft of Encryption Legislation,” apr 2016. [Online]. Available: https://www.burr.senate.gov/press/releases/intelligence-committee-leaders-release-discussion-draft-of-encryption-legislation-

[43] T. May, “The Cyphernomicon: Cypherpunks FAQ and More,” *Cypherpunks*, vol. 0.666, sep 1994. [Online]. Available: https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ

[44] B. Schneier, “Scaring People into Supporting Backdoors - Schneier on Security,” dec 2019. [Online]. Available: https://www.schneier.com/blog/archives/2019/12/scaring_people_.html

[45] E. W. Group and E. W. Group, “Moving the Encryption Policy Conversation Forward.” [Online]. Available: https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573

[46] R. J. Owen, “Law Enforcement’s Dilemma: Fighting 21st Century Encrypted Communications with 20th Century Legislation,” Mar. 2018. [Online]. Available: https://www.hsaj.org/articles/14547

[47] J. Granick, “The FBI’s Gigantic Math Error,” may 2018. [Online]. Available: https://www.aclu.org/blog/national-security/privacy-and-surveillance/fbis-gigantic-math-error

[48] E. Geller, “’Get your act together’: Tech companies face bipartisan congressional uproar over encryption.” [Online]. Available: https://www.politico.com/news/2019/12/10/tech-companies-bipartisan-congress-encryption-080704

[49] L. Graham, "S.3398 - 116th Congress (2019-2020): EARN IT Act of 2020," Mar. 2020. [Online]. Available: https://www.congress.gov/bill/116th-congress/senate-bill/3398

[50] L. H. Newman, "The EARN IT Act Is a Sneak Attack on Encryption," *Wired*, mar 2020. [Online]. Available: https://www.wired.com/story/earn-it-act-sneak-attack-on-encryption/

[51] R. Pfefferkorn, "The EARN IT Act: How to Ban End-to-End Encryption Without Actually Banning It," jan 2020. [Online]. Available: https://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it

[52] D. E. Denning and D. K. Branstad, "A taxonomy for key escrow encryption systems," *Communications of the ACM*, vol. 39, no. 3, pp. 34–40, Mar. 1996. [Online]. Available: http://portal.acm.org/citation.cfm?doid=227234.227239

[53] M. Blaze, "Oblivious key escrow," in *Information Hiding*, G. Goos, J. Hartmanis, J. Leeuwen, and R. Anderson, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, vol. 1174, pp. 335–343. [Online]. Available: http://link.springer.com/10.1007/3-540-61996-8_50

[54] C. Boyd, X. Boyen, C. Carr, and T. Haines, "Key Recovery: Inert and Public," in *Paradigms in Cryptology – Mycrypt 2016. Malicious and Exploratory Cryptology*, R. C.-W. Phan and M. Yung, Eds. Cham: Springer International Publishing, 2017, vol. 10311, pp. 111–126. [Online]. Available: http://link.springer.com/10.1007/978-3-319-61273-7_6

[55] S. Servan-Schreiber and A. Wheeler, "Judge, Jury & Encryptioner: Exceptional Device Access with a Social Cost," *arXiv:1912.05620 [cs]*, Mar. 2020, arXiv: 1912.05620. [Online]. Available: http://arxiv.org/abs/1912.05620

[56] S. Savage, "Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. Toronto Canada: ACM, Jan. 2018, pp. 1761–1774. [Online]. Available: http://dl.acm.org/doi/10.1145/3243734.3243758

[57] R. Ozzie, “rayozzie/clear.” [Online]. Available: https://github.com/rayozzie/clear

[58] M. Bellare and R. L. Rivest, *Translucent cryptography: an alternative to key escrow and its implementation via fractional oblivious transfer*. Cambridge, Mass.: Massachusetts Institute of Technology. Laboratory for Computer Science, nov 1996, oCLC: 37685990.

[59] C. Wright and M. Varia, “Crypto Crumple Zones: Enabling Limited Access without Mass Surveillance,” in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. London: IEEE, Apr. 2018, pp. 288–306. [Online]. Available: https://ieeexplore.ieee.org/document/8406606/

[60] H. Y. Nguyen, “Lawful Hacking: Toward a Middle-Ground Solution to the Going Dark Problem,” Naval Postgraduate School Monterey United States, Tech. Rep., Mar. 2017. [Online]. Available: https://apps.dtic.mil/docs/citations/AD1045945

[61] S. Soesanto, *No middle ground: Moving on from the crypto wars*. European Council on Foreign Relations, jul 2018. [Online]. Available: https://www.ecfr.eu/publications/summary/no_middle_ground_moving_on_from_the_crypto_wars

[62] S. Bittenbender, “Pa. Court: Suspect Can’t Be Compelled To Reveal Password.” [Online]. Available: https://www.mcheraldonline.com/story/2019/12/05/news/pa-court-suspect-cant-be-compelled-to-reveal-password/3391.html

[63] N. Sobel, “The Massachusetts High Court Rules That State Can Compel Password Decryption in Commonwealth v. Jones,” Apr. 2019. [Online]. Available: https://www.lawfareblog.com/massachusetts-high-court-rules-state-can-compel-password-decryption-commonwealth-v-jones

[64] A. Greenberg, “How Dutch Police Took Over Hansa, a Top Dark Web Market,” *Wired*, mar 2018. [Online]. Available: https://www.wired.com/story/hansa-dutch-police-sting-operation/

[65] U. Congress, "28 U.S. Code § 1651 - Writs," 1789. [Online]. Available: https://www.law.cornell.edu/uscode/text/28/1651

[66] J. Feigenbaum and D. J. Weitzner, "On the Incommensurability of Laws and Technical Mechanisms: Or, What Cryptography Can't Do," in *Security Protocols XXVI*, V. Matyáš, P. Švenda, F. Stajano, B. Christianson, and J. Anderson, Eds. Cham: Springer International Publishing, 2018, vol. 11286, pp. 266–279. [Online]. Available: http://link.springer.com/10.1007/978-3-030-03251-7_31

[67] J. Madison and G. Mason, "The Bill of Rights: A Transcription," Dec. 1791. [Online]. Available: https://www.archives.gov/founding-docs/bill-of-rights-transcript

[68] T. E. Morgan, "H.R.13680 - 94th Congress (1975-1976): An Act to amend the Foreign Assistance Act of 1961 and the Foreign Military Sales Act, and for other purposes." Jun. 1976. [Online]. Available: https://www.congress.gov/bill/94th-congress/house-bill/13680

[69] R. W. Kastenmeier, "H.R.4952 - 99th Congress (1985-1986): Electronic Communications Privacy Act of 1986," Oct. 1986. [Online]. Available: https://www.congress.gov/bill/99th-congress/house-bill/4952

[70] D. Edwards, "H.R.4922 - 103rd Congress (1993-1994): Communications Assistance for Law Enforcement Act," Oct. 1994. [Online]. Available: https://www.congress.gov/bill/103rd-congress/house-bill/4922

[71] R. Pfefferkorn, "Thoughts on the Senate Judiciary Committee's Hearing on Encryption," dec 2019. [Online]. Available: https://cyberlaw.stanford.edu/blog/2019/12/thoughts-senate-judiciary-committee%E2%80%99s-hearing-encryption

[72] S. Reyes, "H.R.6304 - 110th Congress (2007-2008): FISA Amendments Act of 2008," Jul. 2008. [Online]. Available: https://www.congress.gov/bill/110th-congress/house-bill/6304

[73] J. Sensenbrenner, "H.R.2048 - 114th Congress (2015-2016): USA FREEDOM Act of 2015," Jun. 2015. [Online]. Available: https://www.congress.gov/bill/114th-congress/house-bill/2048

[74] C. Administration, "Cyberspace Electronic Security Act of 1999," sep 1999. [Online]. Available: https://epic.org/crypto/legislation/cesa/bill_text.html

[75] P. J. Leahy, "S.3083 - 106th Congress (1999-2000): Enhancement of Privacy and Public Safety in Cyberspace Act," Sep. 2000. [Online]. Available: https://www.congress.gov/bill/106th-congress/senate-bill/3083

[76] U. Senate, "Congressional Record," sep 2000. [Online]. Available: https://www.congress.gov/congressional-record/2000/9/20/senate-section/article/S8823-1

[77] Z. Lofgren, "H.R.5823 - 115th Congress (2017-2018): Secure Data Act of 2018," Jul. 2018. [Online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/5823

[78] T. Lieu, "H.R.4170 - 116th Congress (2019-2020): ENCRYPT Act of 2019," Sep. 2019. [Online]. Available: https://www.congress.gov/bill/116th-congress/house-bill/4170

[79] L. Graham, T. Cotton, and M. Blackburn, "Graham, Cotton, Blackburn Introduce Balanced Solution to Bolster National Security, End Use of Warrant-Proof Encryption that Shields Criminal Activity | United States Senate Committee on the Judiciary," jun 2020. [Online]. Available: https://www.judiciary.senate.gov/press/rep/releases/graham-cotton-blackburn-introduce-balanced-solution-to-bolster-national-security-end-use-of-warrant-proof-encryption-that-shields-criminal-activity

[80] M. M. Feeley and E. L. Rubin, *Judicial policy making and the modern state: how the courts reformed America's prisons*, ser. Cambridge criminology series. Cambridge: Cambridge Univ. Press, 2000, oCLC: 833732873.

[81] S. B. Franklin, “Carpenter and the End of Bulk Surveillance of Americans,” Jul. 2018. [Online]. Available: https://www.lawfareblog.com/carpenter-and-end-bulk-surveillance-americans

[82] A. Gidari, “CALEA Limits the All Writs Act and Protects the Security of Apple’s Phones,” feb 2016. [Online]. Available: /blog/2016/02/calea-limits-all-writs-act-and-protects-security-apples-phones

[83] T. B. Lee, “NJ Supreme Court: No 5th Amendment right not to unlock your phone,” Aug. 2020. [Online]. Available: https://arstechnica.com/tech-policy/2020/08/nj-supreme-court-no-5th-amendment-right-not-to-unlock-your-phone/

[84] ——, “It’s unconstitutional for cops to force phone unlocking, court rules,” Jun. 2020. [Online]. Available: https://arstechnica.com/tech-policy/2020/06/indiana-supreme-court-its-unconstitutional-to-force-phone-unlocking/

[85] L. Vaas, “Court says suspect can’t be forced to reveal 64-character password,” Nov. 2019. [Online]. Available: https://nakedsecurity.sophos.com/2019/11/26/court-says-suspect-cant-be-forced-to-reveal-64-character-password/

[86] L. Acosta, K. Buchanan, N. Boring, E. Soares, T. Ahmad, T. Papademetriou, J. Gesley, R. Levush, S. Umeda, H. Goitom, E. Hofverberg, L. Zhang, and C. Feikert-Ahalt, “Government Access to Encrypted Communications,” May 2016. [Online]. Available: https://www.loc.gov/law/help/encrypted-communications/gov-access.pdf

[87] J. A. Lewis, D. E. Zheng, and W. A. Carter, “The Effect of Encryption on Lawful Access to Communications and Data,” feb 2017. [Online]. Available: https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data

[88] NSA, “Ukusa Agreement Release,” 2020. [Online]. Available: https://www.nsa.gov/news-features/declassified-documents/ukusa/

[89] U. Legislature, “Investigatory Powers Act 2016,” 2016. [Online]. Available: http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

[90] AG, “Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018,” 2018. [Online]. Available: https://www.legislation.gov.au/Details/C2018A00148/Html/Text,http://www.legislation.gov.au/Details/C2018A00148

[91] C. Parsons, “Canada’s New and Irresponsible Encryption Policy: How the Government of Canada’s New Policy Threatens Charter Rights, Cybersecurity, Economic Growth, and Foreign Policy,” Aug. 2019. [Online]. Available: https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/

[92] J. L. Donahue, “A comparative analysis of international encryption policies en route to a domestic solution,” Thesis, Monterey, California: Naval Postgraduate School, Mar. 2018. [Online]. Available: https://calhoun.nps.edu/handle/10945/58291

[93] A. P. S. Commission, “Tackling wicked problems : A public policy perspective,” Mar. 2018. [Online]. Available: https://www.apsc.gov.au/tackling-wicked-problems-public-policy-perspective

[94] L. C. Evans, Michael, “Arrests after Blackberry cracked five years after seizure,” Aug. 2020. [Online]. Available: https://www.smh.com.au/national/nsw/silver-bullet-mass-arrests-after-blackberry-cracked-five-years-after-seizure-20200731-p55hbq.html

[95] J. Baker, “Rethinking Encryption,” *Lawfare*, Oct. 2019. [Online]. Available: https://www.lawfareblog.com/rethinking-encryption

[96] C. E. Lindblom, “The Science of ”Muddling Through”,” *Public Administration Review*, vol. 19, no. 2, p. 79, 1959. [Online]. Available: https://www.jstor.org/stable/973677

[97] J. Wolff, "The Computer Fraud and Abuse Act Is 30 Years Old. It's More Confusing Than Ever." Sep. 2016. [Online]. Available: https://slate.com/technology/2016/09/the-computer-fraud-and-abuse-act-turns-30-years-old.html

[98] A. Etzioni, "Mixed-Scanning: A "Third" Approach to Decision-Making," *Public Administration Review*, vol. 27, no. 5, p. 385, Dec. 1967. [Online]. Available: https://www.jstor.org/stable/973394

[99] C. R. Sunstein, "Beyond Cheneyism and Snowdenism," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2589636, Apr. 2015. [Online]. Available: https://papers.ssrn.com/abstract=2589636

[100] W. S. Angerman, "Coming full circle with boyd's ooda loop ideas: An analysis of innovation diffusion and evolution," AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH SCHOOL OF ENGINEERING AND …, Tech. Rep., 2004. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a425228.pdf

[101] B. Schneier, "The Future of Incident Response," *IEEE Security Privacy*, vol. 12, no. 5, pp. 96–96, Sep. 2014.

[102] A. Rozenshtein, "Child Exploitation and the Future of Encryption," Oct. 2019. [Online]. Available: https://www.lawfareblog.com/child-exploitation-and-future-encryption

[103] Committee on Law Enforcement and Intelligence Access to Plaintext Information, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, and National Academies of Sciences, Engineering, and Medicine, *Decrypting the Encryption Debate: A Framework for Decision Makers*. Washington, D.C.: National Academies Press, May 2018. [Online]. Available: https://www.nap.edu/catalog/25010

[104] A. Renton and A. Macintosh, "Computer-Supported Argument Maps as a Policy Memory," *The Information Society*, vol. 23, no. 2, pp. 125–133, Mar. 2007. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/01972240701209300

[105] S. J. B. Shum, A. M. Selvin, M. Sierhuis, J. Conklin, C. B. Haley, and B. Nuseibeh, "Hypermedia Support for Argumentation-Based Rationale," in *Rationale Management in Software Engineering*, A. H. Dutoit, R. McCall, I. Mistrík, and B. Paech, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 111–132. [Online]. Available: http://link.springer.com/10.1007/978-3-540-30998-7_5

[106] W. Kunz, H. W. J. Rittel, W. Messrs, H. Dehlinger, T. Mann, and J. J. Protzen, "Issues as elements of information systems," Tech. Rep., 1970. [Online]. Available: http://www-iurd.ced.berkeley.edu/pub/wp-131.pdf

[107] J. Conklin and M. L. Begeman, "gIBIS: a hypertext tool for exploratory policy discussion," in *Proceedings of the 1988 ACM conference on Computer-supported cooperative work - CSCW '88*. Portland, Oregon, United States: ACM Press, oct 1988, pp. 140–152. [Online]. Available: http://dl.acm.org/citation.cfm?doid=62266.62278

[108] C. Voigt, "Argdown," 2018. [Online]. Available: https://argdown.org/

[109] M. Varia, "A Roadmap for Exceptional Access Research," Dec. 2018. [Online]. Available: https://www.lawfareblog.com/roadmap-exceptional-access-research

[110] O. Liebermann, "How a hacked phone may have led killers to Khashoggi," jan 2019. [Online]. Available: https://www.cnn.com/2019/01/12/middleeast/khashoggi-phone-malware-intl/index.html

[111] P. Rogaway, "The Moral Character of Cryptographic Work," Cryptology ePrint Archive, Tech. Rep. 1162, dec 2015. [Online]. Available: https://eprint.iacr.org/2015/1162

[112] FBI, "Lawful Access," 2020. [Online]. Available: https://www.fbi.gov/about/leadership-and-structure/science-and-technology-branch/lawful-access

[113] R. Goodale, J. Wilson-Raybould, A. Hussen, G. Brandis, P. Dutton, C. Finlayson, M. Woodhouse, A. Rudd, J. Kelly, and J. Sessions, "Five Country Ministerial 2017: Joint

Communiqué," Jun. 2017. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fv-cntry-mnstrl-2017/index-en.aspx

[114] L. K. Johnson, "Congressional Supervision of America's Secret Agencies: The Experience and Legacy of the Church Committee," *Public Administration Review*, vol. 64, no. 1, pp. 3–14, Jan. 2004. [Online]. Available: http://doi.wiley.com/10.1111/j.1540-6210.2004.00342.x

[115] D. Barrett, "FBI repeatedly overstated encryption threat figures to Congress, public," may 2018. [Online]. Available: https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html

[116] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R. L. Rivest, J. I. Schiller, and B. Schneier, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," may 1997. [Online]. Available: https://academiccommons.columbia.edu/doi/10.7916/D8GM8F2W

[117] P. Swire and K. Ahmad, "Encryption and Globalization," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 1960602, Nov. 2011. [Online]. Available: https://papers.ssrn.com/abstract=1960602

[118] L. Koepke, E. Weil, U. Janardan, T. Dada, and H. Yu, "Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones," oct 2020. [Online]. Available: https://www.upturn.org/reports/2020/mass-extraction

[119] Statista, "Most popular messaging apps," oct 2020. [Online]. Available: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

[120] W. Carter, J. Daskal, and W. Crumpler, "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge," jul 2018. [Online]. Available: https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge

[121] D. E. Shelton, Y. S. Kim, and G. Barak, "A Study of Juror Expectations and Demands Concerning Scientific Evidence: Does the 'CSI Effect' Exist?" Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 958224, jan 2006. [Online]. Available: https://papers.ssrn.com/abstract=958224

[122] T. Cushing, "FBI Boss Chris Wray: We Put A Man On The Moon So Why Not Encryption Backdoors?" jul 2018. [Online]. Available: https://www.techdirt.com/articles/20180721/12074340282/fbi-boss-chris-wray-we-put-man-moon-so-why-not-encryption-backdoors.shtml

[123] S. M. Bellovin, M. Blaze, S. Clark, and S. Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2312107, Aug. 2013. [Online]. Available: https://papers.ssrn.com/abstract=2312107

[124] S. Hennessey, "Lawful hacking and the case for a strategic approach to "Going Dark"," Oct. 2016. [Online]. Available: https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/

[125] A. Feuer, "El Chapo Trial: How a Colombian I.T. Guy Helped U.S. Authorities Take Down the Kingpin," *The New York Times*, Jan. 2019. [Online]. Available: https://www.nytimes.com/2019/01/08/nyregion/el-chapo-trial.html

[126] D. Goodin, "Zeroday exploit prices are higher than ever, especially for iOS and messaging apps," Jan. 2019. [Online]. Available: https://arstechnica.com/information-technology/2019/01/zeroday-exploit-prices-continue-to-soar-especially-for-ios-and-messaging-apps/

[127] M. Green, "A few thoughts on Ray Ozzie's "Clear" Proposal," Apr. 2018. [Online]. Available: https://blog.cryptographyengineering.com/2018/04/26/a-few-thoughts-on-ray-ozzies-clear-proposal/

[128] I. Levy and R. Crispin, "Principles for a More Informed Exceptional Access Debate," Nov. 2018. [Online]. Available: https://www.lawfareblog.comhttps://www.lawfareblog.com/principles-more-informed-exceptional-access-debate/principles-more-informed-exceptional-access-debate

[129] J. Callas, "The 'Ghost User' Ploy to Break Encryption Won't Work," jul 2019. [Online]. Available: https://www.aclu.org/blog/privacy-technology/ghost-user-ploy-break-encryption-wont-work

[130] B. Schneier, "Evaluating the GCHQ Exceptional Access Proposal," Jan. 2019. [Online]. Available: https://www.lawfareblog.com/evaluating-gchq-exceptional-access-proposal

[131] E. F. Foundation, "DRM," nov 2020. [Online]. Available: https://www.eff.org/issues/drm

[132] A. Inc., "Apple Platform Security," 2020. [Online]. Available: https://support.apple.com/guide/security/welcome/1/web

[133] E. Tromer, "Eran tromer's attack on ray ozzie's clear protocol." [Online]. Available: https://www.cs.columbia.edu/~smb/blog/2018-05/2018-05-02.html

[134] S. Goldwasser and S. Park, "Public Accountability vs. Secret Laws: Can They Coexist?: A Cryptographic Proposal," in *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society - WPES '17*. Dallas, Texas, USA: ACM Press, oct 2017, pp. 99–110. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3139550.3139565

[135] Ballotpedia, "Michigan Proposal 2, Search Warrant for Electronic Data Amendment (2020)," nov 2020. [Online]. Available: https://ballotpedia.org/Michigan_Proposal_2,_Search_Warrant_for_Electronic_Data_Amendment_(2020)

Grand Valley State University Libraries
ScholarWorks@GVSU Institutional Repository

Thesis Submission Agreement

I agree to grant the Grand Valley State University Libraries a non-exclusive license to provide online **open access** to my submitted thesis ("the Work") via ScholarWorks@GVSU. *You retain all copyright in your work, but you give us permission to make it available online for anyone to read and to preserve it in ScholarWorks@GVSU.*

ScholarWorks@GVSU is an open-access repository maintained by the Grand Valley State University Libraries to showcase, preserve, and provide access to the scholarly and creative work produced by the university community. For more information, email scholarworks@gvsu.edu, or visit our webpage at http://scholarworks.gvsu.edu/about.html.

I warrant as follows:

1 I hold the copyright to this work, and agree to permit this work to be posted in the ScholarWorks@GVSU institutional repository.

2 I understand that accepted works may be posted immediately as submitted, unless I request otherwise.

3 I have read, understand, and agree to abide by the policies of ScholarWorks@GVSU. (Our policies can be found at: http://scholarworks.gvsu.edu/about.html)

By typing my name into the Author field I am agreeing to the terms above and attaching my electronic signature. I understand that if I do not agree to these terms, I should not type my name.

Title of thesis: Confronting Wicked Crypto

Author: Kevin Nicholas Kredit Date: 12/18/20

Embargo Option: *(You may choose to restrict electronic access to your work for up to three years from the date the work is submitted to ScholarWorks. When the embargo expires, your work will automatically become available.)*

Length of Embargo: Three years

Keywords: *(six relevant words to describe the content of your thesis)*

Encryption, Policy, Exceptional Access, Wicked Problems