A COMPARATIVE ANALYSIS OF INTERNATIONAL ENCRYPTION POLICIES EN ROUTE TO A DOMESTIC SOLUTION

by

James L. Donahue

March 2018

Thesis Advisor: Wade Huntley
Second Reader: Robert Simeral

Approved for public release. Distribution is unlimited.
A COMPARATIVE ANALYSIS OF INTERNATIONAL ENCRYPTION POLICIES EN ROUTE TO A DOMESTIC SOLUTION

This thesis examines the encryption policies of Israel and China in an effort to determine whether their respective approaches effectively and reasonably address the issue of law enforcement access to encrypted devices in the United States. The proliferation of encrypted devices poses a growing challenge to law enforcement agencies in their efforts to gather evidence. Meanwhile, an ongoing debate, decades in the making, persists between those arguing for and against easing the means by which the government accesses these encrypted devices. Using qualitative analysis, the thesis assesses the encryption policies of Israel and China in terms of legality, cost, political acceptance, and potential for success in their application within the United States. Based on this analysis, this thesis recommends policymakers give consideration to a solution that resembles Israel’s approach. The characteristics of this model include creating, under existing laws, a centralized forensic laboratory supported by a network of examiners located across the country working to gain access to encrypted devices through vulnerabilities. These efforts would be bolstered by relationships with the private sector and academia. Tailoring the U.S. device encryption approach to be more consistent in structure with that of Israel has the potential to bring the United States closer to a viable domestic solution.
THIS PAGE INTENTIONALLY LEFT BLANK
A COMPARATIVE ANALYSIS OF INTERNATIONAL ENCRYPTION POLICIES EN ROUTE TO A DOMESTIC SOLUTION

James L. Donahue
Assistant to the Special Agent in Charge, United States Secret Service,
Richmond Field Office, Richmond, Virginia
M.A., Argosy University, 2006
B.A., Yale University, 2000

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2018

Approved by: Wade Huntley
Thesis Advisor

Robert Simeral
Second Reader

Erik Dahl
Associate Chair for Instruction
Department of National Security Affairs
THIS PAGE INTENTIONALLY LEFT BLANK
ABSTRACT

This thesis examines the encryption policies of Israel and China in an effort to determine whether their respective approaches effectively and reasonably address the issue of law enforcement access to encrypted devices in the United States. The proliferation of encrypted devices poses a growing challenge to law enforcement agencies in their efforts to gather evidence. Meanwhile, an ongoing debate, decades in the making, persists between those arguing for and against easing the means by which the government accesses these encrypted devices. Using qualitative analysis, the thesis assesses the encryption policies of Israel and China in terms of legality, cost, political acceptance, and potential for success in their application within the United States. Based on this analysis, this thesis recommends policymakers give consideration to a solution that resembles Israel’s approach. The characteristics of this model include creating, under existing laws, a centralized forensic laboratory supported by a network of examiners located across the country working to gain access to encrypted devices through vulnerabilities. These efforts would be bolstered by relationships with the private sector and academia. Tailoring the U.S. device encryption approach to be more consistent in structure with that of Israel has the potential to bring the United States closer to a viable domestic solution.
THIS PAGE INTENTIONALLY LEFT BLANK
TABLE OF CONTENTS

I. INTRODUCTION .....................................................................................................................1
   A. PROBLEM STATEMENT .......................................................................................................1
   B. RESEARCH QUESTION ......................................................................................................4
   C. LITERATURE REVIEW ......................................................................................................5
      1. Encryption and the Debate ...............................................................................................6
      2. A Position for Exceptional Access ...................................................................................7
      3. A Position in Opposition to Exceptional Access ..............................................................10
      4. A Middle Ground Solution? ...........................................................................................13
      5. Beyond the Borders of the United States: China and Israel ...........................................14
   D. RESEARCH DESIGN .........................................................................................................17
   E. CHAPTER OUTLINE ..........................................................................................................18

II. ENCRYPTION AND ITS CHALLENGE TO LAW ENFORCEMENT ...............19
    A. DEVICE ENCRYPTION BACKGROUND ........................................................................20
    B. A BRIEF HISTORY OF ENCRYPTION ...........................................................................21
    C. THE CRYPTO WARS TO PRESENT DAY ....................................................................27
       1. The Clipper Chip ............................................................................................................27
       2. Export Controls of Encryption Items .............................................................................30
       3. Snowden .......................................................................................................................32
    D. THE CHALLENGE FOR U.S. LAW ENFORCEMENT ....................................................34

III. ENCRYPTION POLICY IN ISRAEL ..............................................................................41
    A. THE SOCIOCULTURAL ENVIRONMENT OF ISRAEL ....................................................42
    B. STRUCTURAL DIMENSIONS TO ENCRYPTED DATA EXTRACTION ............................46
       1. Israel Police Cybercrime Unit .......................................................................................46
       2. Partnerships ...................................................................................................................48
    C. ENCRYPTION REGULATORY POLICY AND APPLICABLE LAWS IN ISRAEL ........50
       1. Regulation of Encryption ..............................................................................................50
       2. Civil Liberties and Stored Information in Israel ............................................................53
    D. CONCLUDING THOUGHTS .............................................................................................54

IV. ENCRYPTION POLICY IN THE PEOPLE’S REPUBLIC OF CHINA .............57
    A. THE POLITICAL DESIGN OF THE CHINESE GOVERNMENT AND ITS IMPACT ON ENCRYPTION ..........................................................58
LIST OF FIGURES

Figure 1. Law Enforcement Structure in China ..........................................................60
LIST OF TABLES

Table 1. Encrypted iOS Devices Related to Open Investigations at the Manhattan District Attorney’s Office in 2016 ......................................................... 38
Table 2. Monies Paid by 20 State Police Agencies to Cellebrite from 2010–2016 .............................................................................................................. 83
Table 3. Charted Representation of the Analysis of the Israeli and Chinese Approaches to Encryption Implemented in the United States ................. 107
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AECA</td>
<td>Arms Export Control Act</td>
</tr>
<tr>
<td>AES</td>
<td>advanced encryption standard</td>
</tr>
<tr>
<td>BGU</td>
<td>Ben-Gurion University of the Negev</td>
</tr>
<tr>
<td>CALEA</td>
<td>Communications Assistance for Law Enforcement Act</td>
</tr>
<tr>
<td>CCP</td>
<td>Chinese Communist Party</td>
</tr>
<tr>
<td>CRS</td>
<td>Congressional Research Service</td>
</tr>
<tr>
<td>CSAIL</td>
<td>MIT Computer Science and Artificial Intelligence Laboratory</td>
</tr>
<tr>
<td>DAG</td>
<td>Deputy Attorney General</td>
</tr>
<tr>
<td>DES</td>
<td>data encryption standard</td>
</tr>
<tr>
<td>DHS</td>
<td>United States Department of Homeland Security</td>
</tr>
<tr>
<td>DOJ</td>
<td>United States Department of Justice</td>
</tr>
<tr>
<td>EAA</td>
<td>Export Administration Act</td>
</tr>
<tr>
<td>ECPA</td>
<td>Electronic Communications Privacy Act</td>
</tr>
<tr>
<td>ECTF</td>
<td>electronic crimes task force</td>
</tr>
<tr>
<td>EES</td>
<td>escrowed encryption standard</td>
</tr>
<tr>
<td>EFF</td>
<td>Electronic Frontier Foundation</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FCCU</td>
<td>Federal Computer Crime Unit</td>
</tr>
<tr>
<td>FIPS</td>
<td>federal information processing standards</td>
</tr>
<tr>
<td>FISA</td>
<td>Foreign Intelligence Surveillance Act</td>
</tr>
<tr>
<td>HJC</td>
<td>United States Congress House Committee on the Judiciary</td>
</tr>
<tr>
<td>HRW</td>
<td>Human Rights Watch</td>
</tr>
<tr>
<td>IACP</td>
<td>International Association of Chiefs of Police</td>
</tr>
<tr>
<td>ICT</td>
<td>information and communication technology</td>
</tr>
<tr>
<td>IDF</td>
<td>Israeli Defense Force</td>
</tr>
<tr>
<td>IoT</td>
<td>internet of things</td>
</tr>
<tr>
<td>ISP</td>
<td>internet service provider</td>
</tr>
<tr>
<td>JTAG</td>
<td>Joint Test Action Group</td>
</tr>
<tr>
<td>JTTF</td>
<td>Joint Terrorism Task Force</td>
</tr>
<tr>
<td>LEAF</td>
<td>law enforcement access field</td>
</tr>
</tbody>
</table>
MIT  Massachusetts Institute of Technology
MOC  member of the U.S. Congress
MOD  Ministry of Defense
MPS  Ministry of Public Security [of China]
MSS  Ministry of State Security [of China]
NIST  National Institute of Standards and Technology
NPC  National People’s Congress [of China]
NSA  National Security Agency
OIG  Office of Inspector General
OSCCA  Office of State Commercial Cryptography Administration [of China]
PERF  Police Executive Research Forum
RCFL  regional computer forensic laboratory
RSA  Rivest-Shamir-Adleman [encryption]
SAFE  Security and Freedom through Encryption
SASC  Senate Armed Services Committee
UFED  universal forensic extraction device
U.S.T.R.  United States Trade Representative
VPN  virtual private network
WAPI  WLAN authentication and privacy infrastructure
WLAN  wireless local area network
EXECUTIVE SUMMARY

According to the Pew Research Center, more than 95% of adults in the United States have a cell phone. Digital technology has permeated almost every facet of daily life, and electronic devices are driving this trend. As biometric identification increases and payment systems like Apple Pay proliferate, it is reasonable to believe devices will soon be the proxy for those items, as well. Hardware and software manufacturers are enabling encryption capabilities on many of these devices to protect information from being compromised. While this security is a benefit to many, strong device encryption poses problems for U.S. law enforcement agencies, which have come to rely on data contained on devices in their investigations. The information contained on a device is vast and can be crucial to law enforcement in their investigations. However, the inability of law enforcement to access or see the information on a device due to encryption precludes this retrieval from happening. This concept is known as “going dark.”

The going dark issue is present, prevalent, and growing. In 2016, Federal Bureau of Investigation (FBI) general counsel Jim Baker said that the FBI is able to get the data it needs 87% of the time. In 2017, FBI Director Christopher Wray testified this number dropped to 50% of the time in fiscal year 2017. Emerging from this trend is a renewed, decades-old debate over the means by which the government accesses these encrypted devices. It is a flashpoint between those in law enforcement who generally advocate a...
regimented, industry-supported approach enabling ready access to encrypted data, and technologists and civil libertarians who are opposed to it. Ironically, both groups in the dispute recognize the need for encryption, as well as the need for government access. However, the two are unable to reach a consensus on reasonably meeting both requirements. While the government is locked in debate, the United States lacks a domestic solution to the issue.

This thesis examines and evaluates the primary encryption approaches of Israel and China in an effort to determine whether their respective approaches effectively and reasonably address the issue of access to encrypted devices in ways that could contribute to resolving debate in the United States. Using qualitative analysis, the thesis assesses the encryption approaches of Israel and China in terms of legality, cost, political acceptance, and potential for success for application within the United States. The Israeli model, structural in nature, focuses on the exploitation of encryption and forensic extraction of devices by the Israel Police cybercrime unit; it proved to be a reasonable and potentially effective model for the United States. The Chinese model, a legislative-based solution, compels telecommunications providers to assist with gaining access to devices; it was found to be an unreasonable and ineffective model for the United States. Based on the results of the analysis of available information, this thesis recommends implementing a new initiative in the United States based on the Israeli model.

The success Israel has in the world of encryption and device data extraction is grounded in the Israel Police’s cybercrime unit and its collaborative partnerships with the military, private sector, and academia. The unit has a centralized forensic laboratory, and a network of officers strategically located across the country who specialize in data extraction from electronic devices. The fact that encryption is inherently vulnerable is a key takeaway of this thesis, and Israel’s approach is best suited to take advantage of this weakness. While restructuring U.S. law enforcement in an identical way to Israel is unrealistic, this thesis recommends considering changes to the approach of U.S. law enforcement’s efforts consistent with characteristics of the Israeli model. The United States already has satisfactory legal authorities, with adequate oversight, within which it can leverage means like “lawful hacking” to access devices with this approach. Changes
to U.S. law enforcement efforts include organizing its structure to be collectively and singularly focused on defeating device encryption, staffed with the appropriate personnel, and supported by adequate resources and external partners. This effort can be accomplished by aligning device encryption efforts under the leadership of one federal agency tasked with coordinating the work of federal, state, and local law enforcement partners operating in laboratories across the country in collaboration with partners in the private sector and academia contributing to the mission.

Tailoring the U.S. device encryption approach to implement core features of the Israeli model has the potential to bring the United States closer to a viable domestic solution. Application of the Israeli approach to device encryption issues in the United States is a reasonable solution with a strong likelihood to be effective. Above all, this thesis contributes to a growing body of academic literature supporting a view that continuing a paralytic debate on the issue serves nobody’s interests. The onus is on those who hold absolutist positions in this debate to allow a reasonable and effective solution to be implemented in the United States.
ACKNOWLEDGMENTS

Thank you to my wife and son for their inspiration, support, and patience with this endeavor. Absent their love, encouragement, and understanding, completion of this project and program would not have been possible. I would also like to thank my parents, who instilled in me an unquenchable thirst for learning and selflessly supported all things I have ever set out to accomplish.

I am grateful to the United States Secret Service, especially those in the Office of Government and Public Affairs, the Office of Investigations, and the Richmond Field Office, for allowing me to attend the Naval Postgraduate School. I am hopeful that the knowledge gleaned from this experience will benefit my colleagues and this extraordinary agency going forward.

I would also like to thank my advisors, Wade Huntley and Robert Simeral, for their guidance and assistance.

Lastly, I would like to extend gratitude to my colleagues in CHDS 1611 for a memorable experience. Thank you for the opportunity to be a part of the pack, engaging in productive discourse, and allowing me to see the homeland security project through your eyes.
THIS PAGE INTENTIONALLY LEFT BLANK
I. INTRODUCTION

Smartphones, led by iPhone, have become an essential part of our lives.1

—Tim Cook
CEO, Apple Inc.

A. PROBLEM STATEMENT

According to the Pew Research Center, more than 95 percent of adults in the United States have a cell phone.2 It is unlikely a more common item is in a person’s direct possession other than currency and identification documents. As biometric identification increases and payment systems like Apple Pay proliferate, it is reasonable to believe devices will soon be the proxy for those items as well.3 As a result, a call for strong encryption has arisen to protect this information from being compromised.

Encryption of data is growing in importance and has become a mainstay in topics of security forums across the United States. Encryption is the coded protection of information in the cyber universe accessible only to those with the appropriate keys to view that data. It is used to protect information and can exist in real-time and stored communications. Real-time communications are those live, in-process communications between two entities. Encryption of data in motion is known as end-to-end encryption,

---

3 For the purposes of this thesis, the term, “device” describes portable electronic communication devices like cellular smartphones and tablets.
which is generally a focus of intelligence agencies. Encrypted communications stored on hardware, such as cell phones or applications within the phone, is typically referred to as device encryption. This type of encryption is commonly encountered by law enforcement and the challenge of exploiting this encrypted data at rest in devices is the focus of this thesis.

Strong device encryption poses problems for U.S. law enforcement agencies, which have come to rely on data contained on devices like cell phones in their investigations. This problem will not soon change. The information contained on a cell phone is vast and can include geo-location activity, critical communications, photographs, and applications used to perpetrate crimes. Using this data in their criminal investigations, law enforcement professionals are able to piece together timelines, gather evidence, identify co-conspirators, and prove or disprove alibis. However, the inability of law enforcement to access or see the information on a device due to encryption precludes this retrieval from happening. This concept is known as “going dark.” Technology companies and telecommunications providers are gaining the ability to add encryption to their products at a rapid rate with relative ease. The threat to law enforcement is that

---

4 Law enforcement agencies also rely on information obtained from live, in-process communications, referred to as Title III wire intercepts. However, the use of electronic surveillance is an investigative technique of last resort. Due to the comprehensive legal guidelines that protect citizens from this intrusive technique, and the rigor involved in operating a wire, it is an uncommon law enforcement technique. Moreover, of the 14,500 wiretaps ordered in the country between 2012 and 2015, only 152 encountered encryption; of those 152, only 30 could not ultimately be decrypted, or .2% of the total. On the other hand, law enforcement commonly relies on evidence found on electronic devices. Based on data collected over a six-month period by the FBI published in a report by the Center for Strategic and International Studies in April 2016, the FBI was unable to access 13% of the phones they collected. Meanwhile, between October 2014 and October 2016, the New York County District Attorney’s Office could not access over 33% of the devices in their possession related to crimes. For this primary reason, this thesis will focus on the latter issue. See “Wiretap Reports,” U.S. Courts, accessed June 1, 2017, http://www.uscourts.gov/statistics-reports/analysis -reports/wiretap-reports; James A. Lewis, Denise E. Zheng, and William A. Carter, The Effect of Encryption on Lawful Access to Communications and Data (Washington, DC: Center for Strategic & International Studies, 2017), 13–14, https://cis-s-prod.s3.amazonaws.com/s3fs-public/publication/1702_21_Lewis_EncryptionsEffect_Web.pdf?HQT76OwM4itFrlEl0k6kZajkid5a.r.rE; District Attorney New York County, Third Report of the Manhattan District Attorney’s Office on Smartphone Encryption and Public Safety (New York: Manhattan District Attorney’s Office, 2017), http://manhattanda.org/sites/default/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

these technological advances will leave law enforcement at a significant disadvantage in their mission to protect citizens of this country.

The Federal Bureau of Investigation (FBI) is at the forefront of the issue following a legal battle with Apple over access to an iPhone belonging to one of the perpetrators of a terrorist attack in San Bernardino, California. While the deliberation over the right to privacy versus the right to government access continues in forums across the country, an opportunity has arisen to discuss the future of U.S. policy options. Exceptional access advocates argue a reasonable, obvious solution exists. They believe that at some reasonable level, given appropriate circumstances, the government does have a right to compel third parties to provide or assist with access to devices that are encrypted.\(^6\) It is obvious because in their view, it is the easiest solution to bypassing device encryption. However, technology companies face scrutiny from a U.S. customer base concerned with privacy, and technology encryption advocates who view these concessions as weakening the security of devices. As a result, the issue is not easily overcome.

While policy professionals and the private sector debate the proper landscape for this answer, advances in encryption continue, and law enforcement organizations struggle to keep up with the number of devices seized for forensic examination that cannot be accessed. Moreover, in some cases, encryption enhancements are occurring outside the walls of major technology companies, which the government typically engages in the debate. The ease and cost of manufacturing devices and applications allows for encryption enhancements that may not include U.S.-based companies subject to agreements or legislation. Even if a resolution with information technology companies is achieved, the United States is in need of a policy solution to this encrypted reality from which law enforcement is able to operate.

In part, because so many prominent technology and communications companies are located in the United States, an expectation exists that an encryption policy will be

---

pioneered in this country. However, despite holding hearings on the issue to address reforms to laws like the Communications Assistance for Law Enforcement Act (CALEA), federal legislators have been unable to reach a satisfactory agreement on a path forward. Meanwhile, representatives from private industry have made it clear they may no longer be interested in assisting U.S. law enforcement.

The issue of data encryption, at rest and in motion, is not exclusive to the United States. The location and transmission of data have few boundaries in the cyber realm. Countries like China and Israel appear to have two different approaches they are already exercising. In China, a counterterrorism law recently passed mandating the support and assistance of telecommunications and internet service providers to support the security activities of the country. This approach differs slightly from Israel, which requires companies with encryption technology to submit to initial regulatory requirements, but does not appear to impose anything further on them down the road. Some have speculated that the more lenient Israeli laws along with the cultural norms of the country allow for technological development and a willingness of cutting-edge companies to voluntarily assist the government. This thesis examines the different paths these countries have taken to grapple with the common challenge in search of lessons that could help advance the U.S. debate about encryption toward a more optimal resolution.

B. RESEARCH QUESTION

Given the need for a solution to the encryption debate in the United States, do the policy options of China or Israel offer models to address the issue of access to encrypted devices effectively and reasonably in the U.S. context?

---


C. LITERATURE REVIEW

University of Virginia Professor Ashley Deeks states, “It is possible to treat encryption as predominantly a rights question, a law enforcement question, an intelligence question, an economic question, or an export control question.” Most literature reviewed more commonly frames encryption as a battle between the right to privacy and the right of the government to exceptional access. This literature review assesses relevant scholarly policy material on this latter debate.

The analysis of the available non-technical literature is separated into distinct categories based on the content of the material. The first section deals with literature that gives a broad description of encryption and the privacy versus exceptional access debate, which has endured largely below the surface of popular media since the 1990s. This section includes the classification of those things considered capable of encryption, namely information at rest and information in transit, as well as the positions staked in a debate with roots many decades old. As a result, the literature reviewed spans this same timeframe in an effort to understand the lack of progress on the topic.

The second section assesses the areas within scholarly material in support of greater government access. This subject matter speaks to the position of law enforcement and intelligence community proponents who advocate for exceptional access to deter and investigate criminal actors and terrorists who may utilize encryption for illicit purposes. The third section describes arguments supporting unfettered encryption and opposing special government access. The point of view maintained by this group ranges from privacy advocates fearful of government intrusion to technology advocates fearful of weakened encryption.

The last section assesses the literature that focuses on the policies of Israel and China. These two countries have implemented different policies without waiting for the United States to act. Further, a review of literature involving encryption in these two

---

countries presents an opportunity to apply the lessons learned to the United States. Their application to the United States in present literature lacks exploration in research to date.

1. Encryption and the Debate

Encryption is the coded protection of information in the cyber universe accessible only to those with the appropriate keys to view that data. It is used to protect information, both lawful and illicit. As discussed informally in the problem statement, scholars agree that encryption is the use of cryptography to protect information existing in two forms, real-time communications and stored communications. Harvard researchers describe the two types as end-to-end encryption and device encryption. Device encryption is the target of this literature review and thesis.

All the reviewed material acknowledges that every effort should be made to have the highest level of encryption to protect information adequately. Former FBI Director James Comey, who was at center of the government’s position on going dark, publicly stated, “The development and robust adoption of strong encryption is a key tool. …We support and encourage the use of secure networks … so as to promote our overall safety.” Cyber scholars representing the view of those in opposition to exceptional access also support this notion, stating there is a “fundamental technical importance of strong cryptography.” The importance and commitment to encryption is clearly undisputed by the parties on either side of the debate.

Regardless of the types of information or importance of encryption, the literature frames an important debate on the issue. While the latest foray into encryption surfaced in mainstream media over the past few years, heavy analysis of positions on encryption

---

11 Berkman Center for Internet and Society at Harvard University, Don’t Panic, Making Progress on the “Going Dark” Debate (Cambridge, MA: Berkman Center for Internet and Society at Harvard University, 2016), 4, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.


had occurred before, in the 1990s. In all literature, it has generally been accepted that it is not a new issue, but instead is a perpetual debate. A Congressional Research Service (CRS) examination of the issue states, “The tension between the benefits and challenges of encryption is not new. It started in the 1990s and was reinvigorated in 2014.” In his comparison of the encryption issue in the 1990s and present day, Matthias Schulze says that

the discursive positions in the two discourses [Clipper and Apple vs. FBI] are somewhat similar. Law enforcement (FBI), intelligence actors (NSA) and politicians (predominantly, but not exclusively conservatives) argue for governmental regulation or encryption and providing exceptional access for legitimate law enforcement inquiries. In both discourses this group produces a relatively homogeneous set of arguments. Technology companies, cryptography experts, scientists and a mix of civil-libertarians and tech enthusiasts argue for widespread, public use of encryption. This group is more heterogeneous and uses a variety of arguments. In both instances, there is a middle ground, recognizing the needs of both groups and arguing for a compromise.

These respective positions and their arguments are explored in the next sections.

2. A Position for Exceptional Access

The literature on encryption reveals many government officials, especially those within law enforcement, maintain the perspective that unlimited encryption is unreasonable. This viewpoint is one side of the debate. These advocates for exceptional access articulate a need for a solution to the issue. Some on this side argue that it should be regulatory in nature. Former FBI Director Comey states, “The Department of Justice believes that the challenges posed by the Going Dark problem are grave, growing, and extremely complex. We believe we will need to pursue multiple paths [for a solution].”

---

14 See Abelson et al. who, in their analysis on the subject, state that the Crypto Wars began in the 1970s, and in many ways, are the same now as they were in the 1990s.


17 United States Senate Committee on the Judiciary, “Going Dark.”
Chairman McCaul of the House Committee on Homeland Security stated to an audience at the U.S. Chamber of Commerce, “Congress has to have a solution to this. There should be international standards and norms, just as there should be with cybersecurity.” The argument of government officials is that an inability to access this information could prevent the deterrence of terrorist attacks or investigation into suspects following criminal acts.

The rationale for the mindset of those in law enforcement who favor a government-brokered approach can be traced to the crutch offered by the CALEA passed in 1994. One of law enforcement’s most valuable tools in an investigation is their ability to listen to telephone communications by “tapping” phone lines following appropriate judicial authorization. In the 1980s and 1990s, telephonic system upgrades included moving from simple-to-tap copper connections to more impenetrable fiber-optics. Law enforcement sought solutions to the interception of these enhanced telephonic communications, commonly known as Title III wiretaps. Ultimately, they relied on legislation to compel telecommunications companies to assist. CALEA outlines the requirements for telecommunications companies to cooperate with the government in the interception of communications following proper authorization from the courts.

Following the passage of CALEA and the advent of enhanced communication through the internet, the government called for alterations that would provide a similar solution of exceptional access. Internet service providers (ISPs) are not included within CALEA. According to Abelson et al., “Claiming that widespread encryption would be disastrous for law enforcement, the U.S. government proposed the use of the Clipper Chip, an encryption device that contained a government master key to give the government access to encrypted communications.” This government-based solution and other attempts were eventually abandoned due to pressure from the technology industry.

---


and the European Union.21 Matthias Schulze states, “The general argument put forward by critics...is that the government should look at the bigger picture, recognizing the general interest of the people and corporations that need encryption, both for privacy reasons but also for business interests and data security.”22 He concludes that the arguments that defeated the Clipper Chip in the 1990s will ultimately prevail in defeating those in favor of exceptional access in the wake of the Apple versus FBI debate today.23

After the Clipper Chip episode, law enforcement and intelligence agencies found other solutions, some of which were described in documents released by Edward Snowden.24 However, following the Snowden disclosures and advances in technology, literature reveals that law enforcement and intelligence agencies are facing renewed challenges with indications that the solution the government is seeking comes in a form that resembles the ease of access afforded by CALEA. In 2012, former FBI Director Mueller testified in front of the Senate Judiciary Committee on the matter of communication on the internet, “What we are seeking is the ability to enforce that [court] order and be able to obtain those communications [transmitted over the Internet], and what we are looking at is some form of legislation.”25 More recently, Director Comey was quoted as saying, “We aren’t seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law.”26 Even some legal scholars, like Richard Posner, who sits on the U.S. Court of Appeals in the Seventh Circuit, has said, “My inclination—it is only that; I am not an expert in these matters—would be to let the NSA have its back door.”27 Literature highlighting

23 Ibid.

9
advocates’ points of view to exceptional access is clear. A solution that compels private industry’s assistance in gaining access is necessary, but the way in which it is achieved remains undefined.

Former FBI Director Comey described a path forward that includes continuing the debate on the issue, observing the privacy rights of citizens, factoring in the international community, and developing novel tools and techniques to address encryption. However, former Director Comey’s talking points are not a solution. Some law enforcement advocates proposed a solution of key escrow, or the secure, third party storage of master keys for authorized decryption, when encryption first became a significant issue of debate in the 1990s. This position has largely not changed, and at that time, experts deemed it an unworthy solution.

Meanwhile, many privacy advocates and cryptography experts who take a contrary position, arguing vehemently against exceptional access, do propose that solution. The next section reviews the literature opposing exceptional access and presents alternative encryption policy directions.

3. A Position in Opposition to Exceptional Access

The other side of the coin in the encryption debate is articulated in a number of documents generated by privacy advocates, security experts, and legal scholars. Their research is supported and published by respected institutions like Harvard, Massachusetts Institute of Technology (MIT), and Northwestern. Within the literature reviewed, authors oppose exceptional access on multiple levels, with some extending beyond the position of privacy. Summarizing the literature on the issue, the arguments are: (1) a fundamental right to privacy is a priority, (2) regulation of exceptional access may lead to increased vulnerabilities, and (3) regulation may prove to be useless since the bounds of encryption will never be defined, and those nefarious characters desiring encryption will just seek it.

---

28 United States Senate Committee on the Judiciary, “Going Dark.”

from those providing it outside of regulated U.S. companies. These arguments are more fully discussed in the following paragraphs.

Privacy is central to the encryption argument. Generally speaking, it is a fundamental right in the United States articulated throughout the Constitution, including the Fourth and Fifth amendments.\textsuperscript{30} Specific to encryption, legal scholar Ashley Deeks, references a report from David Kaye, the United Nations Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression that states, “Encryption and anonymity…create a zone of privacy to protect opinion and belief.”\textsuperscript{31} This report is in reference to the importance of encryption to certain groups of people, especially political activists in countries with authoritarian regimes. Even advocates of exceptional access acknowledge the importance of privacy in the encryption debate. In his testimony to the Senate Judiciary Committee, former FBI Director James Comey says, “it is our obligation to uphold civil liberties, including the right to privacy…the fundamental right of people to engage in private communications, regardless of the medium or technology.”\textsuperscript{32}

Researchers, in literature released by MIT, state that as a result of government regulated encryption for the purposes of access, an increasing number of vulnerabilities to encryption will result with the requirement to maintain encryption keys, increased complexity in systems, and at least one known point of access.\textsuperscript{33} Much of the literature supports their present day arguments through references to a vulnerability exploited during the telephone switch era. Several pieces refer to the Athens Affair, in which a weakness in a phone switch designed for government wiretapping was exploited that

\begin{flushleft}
\textsuperscript{30} U.S. Const. amend. IV and V.
\end{flushleft}

\begin{flushleft}
\end{flushleft}

\begin{flushleft}
\textsuperscript{32} United States Senate Committee on the Judiciary, “Going Dark.”
\end{flushleft}

\begin{flushleft}
\textsuperscript{33} Abelson et al., “Keys under Doormats,” 1–2.
\end{flushleft}
allowed unauthorized individuals to access telephone communications of high-level government officials in Greece.\(^{34}\)

With regards to limiting encryption, Lawrence Lessig states, “From the very start of the debate over the government’s control of encryption, techies have argued that such regulations are silly. Code can always be exported; bits know no borders.”\(^{35}\) One Indian researcher has remarked, “[W]riting a new encrypted app is not exactly rocket science and switching over to apps made in other countries without restrictive regulations will be child’s play.”\(^{36}\) Harvard researchers take the argument about encryption a step further and claim that the “going dark” debate is a misnomer. They claim that although the government is certainly losing some access to information with the implementation of enhanced encryption on some services, the expanded internet of things (IoT) is actually providing greater means of surveillance, not less.\(^{37}\)

That being said, those in opposition to exceptional access do think a need exists for law enforcement to gain access to encrypted devices and communications. In Congressional testimony, Susan Landau says, “Law enforcement is entirely correct that it has a problem….I agree that with the new communications technologies, there is a need for law enforcement access.”\(^{38}\) Their perception to how this access is achieved differs from most exceptional access advocates.

The solution to exceptional access proposed by many encryption advocates boils down to law enforcement and intelligence community responsibility. These authors argue that the onus is on those agencies to overcome their perceived problem with exceptional access. Cyber-security expert Bruce Schneier, in commenting about the FBI’s fight with


\(^{35}\) Lessig, Code: Version 2.0, 1.


\(^{37}\) Berkman Center for Internet and Society at Harvard University, Don’t Panic, 15.

Apple to gain access to the phone of a terrorist in San Bernardino states, “The FBI did the right thing by using an existing vulnerability rather than forcing Apple to create a new one.”

Researchers supported by Northwestern make similar comments in their work claiming, “We are suggesting use of pre-existing vulnerabilities for lawful access to communications.” Those researchers go as far as to say that such a method will always be necessary since the technology behind internet communications is non-traditional, and unlike the uniformity found in telecommunications, it will always be possible that an encrypted technology will exist outside of one governed by a CALEA-like law.

Susan Hennessey of Brookings states, “Lawful hacking is a necessary, though possibly not sufficient, element of a workable solution without mandated exceptional access. [It] should be viewed as the central element of a comprehensive alternative strategy.”

4. A Middle Ground Solution?

The literature reviewed typically favors one side of the debate or the other. Little scholarly research supports a viable middle ground solution. The administration under President Obama recognized the conflict between the two sides described previously. During the South by Southwest Festival in 2016, President Obama stated, “My conclusion so far is that you cannot take an absolutist view on this.”

Hoaithi Nguyen, a graduate of the Center for Homeland Defense and Security at the Naval Postgraduate School, attempted to advance the debate over encryption towards concrete policy proposals in her award winning thesis, “Lawful Hacking: Toward a Middle Ground Solution to the Going Dark Problem.” Nguyen concludes, “Congress

---

40 Bellovin et al., “Lawful Hacking,” 27.  
41 Bellovin et al., 30.  
must act.” She states, “I recommend that policy makers adopt legislative actions to legalize and thereby legitimize hacking by law enforcement in limited cases as a middle-ground solution.”

Nguyen discusses conducting ethical hacking with a lawful warrant that satisfies Fourth Amendment requirements in concert with minimizing procedures and a transparency requirement. She describes this requirement as, “preferable to mandating exceptional access.” However, Nguyen does not articulate what new concrete legislative actions, if any, should be undertaken to achieve this middle ground goal.

5. **Beyond the Borders of the United States: China and Israel**

The issue of encryption is not endemic to the United States. Other countries in the world, like Canada, are standing by waiting for policy decisions to be made in the United States, as they did with CALEA, by piggybacking on the outcome of the debate. Literature indicates that two countries, China and Israel, moved beyond the debate and established policies on the issue of encryption that fit the values and cultures of their respective governments and those in the population supporting that government. A review of this literature also reveals that prior efforts have not been taken to apply the lessons learned in those countries to the issue of device encryption in the United States.

a. **China**

Hoover Institute researcher Adam Segal’s historical analysis in *China, Encryption Policy, and International Influence* describes forceful efforts through the State Encryption Management Bureau to regulate and legislate encryption. Efforts started in the late 1990s and most recently culminated with the passage of China’s 2016 counter-

---


45 Nguyen, 75.

46 Nguyen, 75.

terrorism law on the issue. The government initially took aim at encryption and early draft versions indicated a requirement for backdoor access and the filing of encryption solutions. However, this approach ultimately changed. According to Bloomberg News, “[The law] that takes effect in June 2017 requires Internet operators to cooperate with investigations involving crime and national security, and imposes mandatory testing and certification of computer equipment. Companies must also give government investigators full access to their data if wrong-doing is suspected.” In the law that passed, Segal states that the foreign community welcomed the exclusion of backdoor and encryption solution requirements, but, “The wording of Article 18 [of the 2016 counter-terrorism act] seems to leave local and state authorities with ‘broad discretionary authority to require companies to provide access to their equipment and decryption support in particular cases.’”

Although China faced some criticism for this law from foreign governments and companies, Segal points out, “The importance of the Chinese market to current revenues and future growth may lead [foreign] firms to fork their technologies, creating different products for different markets.” Domestic companies, like Huawei and Xiaomi, are also described as being increasingly reliant on the Chinese government’s support for future growth. The authors’ descriptions indicate that China’s decision is a feasible course of action, values and human rights notwithstanding.

b. Israel

Israel’s encryption laws were established decades ago under Israel’s Ministry of Defense. Attorneys Matthew Waxman and Doron Hindin provide one of the only critical


51 Segal, 8.

52 Segal, 9.
analyses of the evolution of Israeli encryption policy and the advantages it provides to the state and information technology firms. According to the attorneys:

Israel has adopted a much farther-reaching regulatory system that effectively governs all forms of “engagement in encryption”... At the same time, the Israeli encryption control mechanisms operate without directly legislating any form of encryption-key depositories, built-in back or front door access points, or other similar requirements. Instead, Israel’s system emphasizes smooth initial licensing processes and cultivates government-private sector collaboration. These processes help ensure that Israeli authorities are apprised of the latest encryption and cyber developments and position the government to engage effectively with the private sector when national security risks are identified.\(^{53}\)

In its governance of all forms of engagement with encryption, the regulatory system in Israel shares similarities with China. The authors explain that the system also affords licensing exemptions, rarely includes direct enforcement, and ultimately, allows for enhanced private sector collaboration with the government.\(^{54}\) One argument raised in the literature is, “An approach that simply mandated all companies deposit encryption keys or create concealed access points would probably undermine this initial dialogue.”\(^{55}\)

The authors do broach an important topic within their analysis that focuses on the socio-cultural differences of Israel from other countries. The government’s close ties with its businesses are often rooted in the compulsory military service completed by the owners of these companies. Further, once established, these businesses often recruit individuals who have excelled in the intelligence and technology sectors of the military. The authors suggest that the lack of an encryption issue in Israel may be the result of a close, working relationship between the government and private sector encouraged by the regulatory practices of the Ministry of Defense. However, they also imply that the socio-cultural norms of the country “facilitate an encryption regime that operates less out of tough enforcement and more through dialogue and mutual assistance between private tech companies and government national security entities.”\(^{56}\) As a result, encryption

\(^{53}\) Waxman and Hindin, “How Does Israel Regulate Encryption.”

\(^{54}\) Waxman and Hindin.

\(^{55}\) Waxman and Hindin.

\(^{56}\) Waxman and Hindin.
technology has flourished in Israel, and in 2014, it was estimated that the country sold 10% of the global encryption and cyber technologies.\textsuperscript{57}

D. RESEARCH DESIGN

The United States has been engaged in an encryption debate for at least 25 years.\textsuperscript{58} Law enforcement leaders tout a solution in which Silicon Valley companies come to the assistance of the U.S. government.\textsuperscript{59} On the other side of the argument, privacy and technology advocates favor a solution generated at the hands of law enforcement.\textsuperscript{60} By all appearances, the quest for a solution is perpetual. A policy gap exists to address the issue while technological devices with encrypted data that may hold evidence stack up in local law enforcement agencies unable to be accessed.\textsuperscript{61} Meanwhile, private enterprises continue to develop devices and technology that utilize encryption, to which advances are being made at a rapid rate. Some countries have accepted this situation as reality and have moved unilaterally to address the issue.

This thesis closely examines the policies of Israel and China because, unlike the United States, both countries have defined approaches to addressing device encryption and these countries lack the public discourse that would otherwise indicate a lack of agreement for their respective approaches. Further, the basis for their approaches mirrors the two sides of the U.S. encryption debate, one favoring structure and resources, and the other, a legal mandate. Given these characteristics, these countries offer policy models relevant to the development of a U.S. domestic solution. The goal of this thesis is to evaluate the disparate policies established by the Israeli and Chinese governments in an effort to glean lessons and potential solutions for a path forward on the issue of device encryption in the United States.

\textsuperscript{57} Waxman and Hindin.

\textsuperscript{58} Abelson et al., “Keys under Doormats,” 5.

\textsuperscript{59} United States Senate Committee on the Judiciary, “Going Dark.”

\textsuperscript{60} Hennessey, “Lawful Hacking and the Case for a Strategic Approach to ‘Going Dark.’”

The thesis examines the historical development and current encryption policy on data at rest in Israel and China using available information in literature. It evaluates the policies using qualitative analysis to assess indicators of legality, cost, political acceptance, and potential for success of each model’s application within the United States. In assessing the respective policies for legality, this thesis evaluates the constitutional and legal implications for implementation. Cost is assessed on two levels, the anticipated impact on government expenditures and repercussions for U.S. businesses. Political acceptance of the policies is evaluated on the expected reception of two groups, the legislative branch and the U.S. population. In assessing the policies for the potential for success, this thesis evaluates the effectiveness of the respective approaches in two areas, resolving the exceptional access debate and the probability of law enforcement to obtain usable data from a device that uses encryption.

E. CHAPTER OUTLINE

The goal of the thesis is to present policy recommendations in the United States relative to device encryption that can serve as a means to end the current debate on the subject. Chapter I presents the problem statement, research question, and reviews the relevant literature on the subject. Chapter II provides a brief history of encryption, the genesis of the debate, and examines the issue of device encryption and the rationale for the necessity of a solution. Chapters III and IV provide background to the policies of Israel and China, respectively. Chapter V evaluates the respective approaches of the two countries using qualitative analysis to assess indicators of legality, cost, political acceptance, and potential for success in the context of an U.S. implementation. Chapter VI contains conclusions and recommendations based on the results of the previous chapters’ policy analyses.
II. ENCRYPTION AND ITS CHALLENGE TO LAW ENFORCEMENT

Apple and Google came out with these softwares [sic] that I can no longer be [un]encrypted by the police... [i]f our phone[s are] running on iOS8 software, they can’t open my phone. This may be [a]nother gift from God.62

—Defendant on a Recorded Prison Phone
Manhattan District Attorney’s Office

That is not a gift from God, but an unintended gift from two of the largest technology companies in the world.63

—Cyrus Vance, Jr.,
District Attorney for Manhattan

The focus of this thesis is on the device encryption approaches of foreign countries to provide recommendations for potential solutions to the problems law enforcement agencies face in the United States. Prior to assessing these policies and providing recommendations, a general discussion on encryption and the mounting problems facing law enforcement will be instructive to the reader. The encryption debate from the government’s point of view commonly revolves around intelligence agencies and their inability to intercept communications. A compelling theoretical argument is that this inability will lead to a catastrophic terrorist attack within the United States that may otherwise be stopped with exceptional access to encrypted communications. This thesis does not argue that it is not a possibility; it is an important issue for intelligence agencies. However, the volume of devices with inaccessible data seized by local, state, and federal


63 United States Senate Committee on Armed Services.
law enforcement in criminal cases on a daily basis is concrete and growing in size each year.

This chapter establishes a common launching point for the discourse to follow. What is device encryption, how did we get to this point, why is it that it has turned into an unending debate, and is the issue really as insurmountable as government experts lead people to believe? Understanding the answers to these questions is the first step in moving towards a solution.

This chapter starts with a brief history on device encryption to familiarize readers on a subject that can otherwise be considered esoteric. While the technical aspects behind encryption are complex and are not the subject of this thesis, a discussion of fundamentals through its evolution does hold value. The fact that encryption is inherently vulnerable to being defeated becomes evident with such an examination. The chapter then moves to a short conversation about the initial encryption debate and significant historical markers since that time to set the foundation for present-day issues. Finally, the chapter concludes with the challenges facing U.S. law enforcement. Establishing the tangible problem of device encryption to law enforcement in the United States prompts the obvious questions of does this issue occur elsewhere in the world? If so, how is it that other countries have chosen to tackle it? These questions are only obvious if the problem of device encryption is properly illustrated as a concern in the United States.

A. DEVICE ENCRYPTION BACKGROUND

In the United States, 95% of Americans own a cell phone and 77% of those cellular devices are smartphones. The companies manufacturing these devices and accompanying operating systems of the phones, like Apple and Google, are focusing on protecting the information contained on the devices. An effort is being made to appeal to their customers’ desires for security and privacy. These companies accomplish this task using encryption.

---

64 Pew Research Center, “Mobile Fact Sheet.”
On a superficial level, device encryption is an integrated process involving the device’s hardware and software, and is initiated when the device is locked. When locked, the device’s operating system then applies a mathematical algorithm to the data on the mobile device that alters the data’s appearance and renders much of the user’s information stored on the phone unreadable in the form of a cipher. The process is reversed when the device is unlocked. The unlocking procedure is initiated with the application of a key, typically activated by a numeric or alpha-numeric passcode, or biometric feature. It should be noted that the owner of the device, in addition to anyone else who has the knowledge of the passcode or has ability to crack the key that unlocks the device, can successfully complete the unlocking procedure.

As a result of encryption, data residing on a device cannot be usefully accessed unless it is decrypted. While encryption can be applied to information at rest or in motion, device encryption is limited to this data at rest. As previously discussed, this thesis focuses on the encryption of the data on a device at the most basic level; that is to say, a locked device utilizing encryption. However, this data at rest can be further delineated to describe data on a locked device beyond the applications installed by the manufacturer in the factory settings, and can include third-party applications, and in most cases, backup images of the device found on cloud storage services. Recognition of these additional characteristics is important to a fuller understanding of the encryption issue, but the conversation is moot if the device is locked and the information within it, encrypted. Equally important to a discussion about device encryption policy is gaining a better historical perspective to understand the central issue of this thesis and persistent vulnerabilities of encryption itself.

B. A BRIEF HISTORY OF ENCRYPTION

Device encryption is part of the evolution of cryptography, which is developed to secure electronic communications and information. The goal of cryptography has always been to hide a communication without allowing that communication to betray its meaning. The hope is that the cipher is strong enough to prevent decryption in a reasonable amount of time. However, history illustrates that methods of cryptography,
with few exceptions, have always been defeated. In 1976, Diffie and Hellman, in their landmark paper on encryption, state, “Experience has shown, however, that few systems can resist the concerted attack of skillful cryptoanalysts, and many supposedly secure systems have subsequently been broken.”

For this reason, the history of encryption is an important backdrop to this thesis. A historical analysis illuminates the vulnerabilities of encryption at almost every intersection in its evolution.

The Caesar Cipher, dating to 58 B.C., is the first reported use of a systematic, mathematical method to mask the symbols used in communications for the purposes of security. Julius Caesar used a simple substitution cipher in his correspondence to preclude unauthorized individuals from reading it. This practice of uniformly shifting all letters of a document up or down a predetermined number of letters within an alphabet was used for hundreds of years to defeat prying eyes. This rudimentary method of secrecy was overcome through something called frequency analysis. In 800 A.D., a mathematician named al Kindi developed the concept of frequency analysis to decipher messages. He postulated that letters of a language appear within a given text at a set percentage. By applying that percentage to text using a substitution cipher, the shift can be determined, which effectively cracks the cipher.

Following the exploited weakness of the substitution cipher, the polyalphabetic cipher met the needs of those seeking to advance their ability to conceal the content of messages. This method, attributed to Leon Battista Alberti in 1467, relies on multiple shifts within an alphabet to secrete the content. One common way to execute this cipher is to use a key word known only to the sender and recipient. The key word coordinates the shift within the alphabet in the message. This type of cipher was still susceptible to

---


frequency analysis and could be cracked after finding repeated series of letters in the text.⁶⁷

Regardless of the weakness of the polyalphabetic cypher, for 400 years, it was the method of choice for strong cryptography. It was not until random shifts were introduced that the evolution of cryptography was furthered. By choosing shifts at random, between one and 26, cryptographers achieved uniform frequency distribution and a lack of repetition. Each letter being encrypted could be one of 26 choices to make brute force attempts to hack a message almost impossible. Each letter in a message could have 26 possibilities; thus, a word longer than one letter would have an unpredictable sequence that grows exponentially by a factor of 26 for each new letter.⁶⁸ The method by which this cipher was passed was through a one-time pad to which both the sender and receiver of a message had access. Frequency analysis proved useless and it ultimately became a precursor for the Enigma Machine, a rotor encryption machine used by the Germans in World War I to share strategic messages by automating this one-time pad.

The means by which the Enigma functioned could be a thesis unto itself, and the one-time pad basis for it was studied extensively. In 1945, Claude Shannon provided mathematical proof that the one-time pad was perfectly secret in a comprehensive classified paper on the subject that was made public in 1949.⁶⁹ At a high level, the Enigma contained four rotors numbered one to 26 that could be set up to elicit millions of different possibilities in the encryption of messages. The Allies cracked the machine when they developed a machine called the Bombe that could test hundreds of thousands of rotor settings in seconds. Their efforts were successful not because of a failure of the one-time pad, but a combination of human errors to include biased decision-making amongst Enigma operators, the recovery of codebooks from a German U-Boat, and an

---


⁶⁸ A six-letter word would have over 308 million possible six-letter sequences.

engineering flaw in the construction of the machine itself. This ability to crack a cryptographic code by exploiting something other than the code itself is an important theme that transcends methods of encryption and is discussed later in this thesis.

This is not to say the one-time pad was infallible. Multiple problems with it have resulted, including the need for it to be lengthy for it to be successful. It also required that two parties had to exchange physically the key to be used to decrypt the message. As the name infers, a one-time pad can only be used one time and a new key must be developed and exchanged for each use. Some of these challenges were overcome with the advent of computing power and the evolution of technology. Following World War II, finance and defense sectors drove rapid advances in cryptography and helped usher in modern encryption. The Cold War between the United States and Russia triggered an arms race along with commensurate defensive measures. Within these means to counter-assault attacks were computerized radar stations that communicated their information to military command centers. Meanwhile, banks became reliant on computers to track and store financial information. Financial transfers once made in person began to occur more frequently domestically using phone lines, and internationally through submarine cables. The banking and defense industries relied on security within their computers and networked communications. Encryption of these devices and their communications were of paramount concern and became the focus of academia.

In 1976, Whitfield Diffie and Martin Hellman, in their paper, *New Directions in Cryptography*, developed a way to allow for encryption and decryption without requiring the physical exchange of a key. According to Diffie and Hellman, “In order to use cryptography to insure privacy, however, it is currently necessary for communicating parties to share a key which is known to no one else. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.” Using an algorithm based on discrete logarithmic functions of prime numbers, Diffie and Hellman illustrated the idea of a public key

---


exchange that could be used to establish privacy and authentication of anyone communicating by way of computers, which is now known as the Diffie-Hellman key exchange. Their use of algorithms in encryption is the basis for cryptographic methods used on modern-day devices.

Contemporaneous to Diffie and Hellman’s efforts, the U.S. National Bureau of Standards recognized the same need for the government to protect information on computers that the researchers addressed for businesses and non-governmental entities. They sought a cipher that would adequately protect this information. A team from IBM pioneered what eventually became known as the data encryption standard (DES) that was adopted by the U.S. government in 1976. According to the Federal Information Processing Standards Publication, “The Data Encryption Standard specifies an algorithm to be implemented in electronic hardware devices and used for the cryptographic protection of computer data...the algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key…the key consists of 64 binary digits [or bits].” The encryption space, or possible combinations for the correct key, consists of over 70 quadrillion options. However, in the 1990s, it was publicly revealed that DES could be cracked in a brute-force attack in under a day’s time.

In 2002, the U.S. National Institute of Standards and Technology (NIST) introduced the advanced encryption standard (AES). It was described as, “A symmetric block cipher that can encrypt and decrypt information...The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.” The encryption space with 128 bit AES is well above $3.4 \times 10^{38}$

---


73 United States National Bureau of Standards, 3.


combinations. Other advances in encryption have been made, such as Rivest-Shamir-Adleman (RSA) asymmetric encryption, but AES is the standard used by the government and many U.S. manufacturers of electronic data storage devices today. AES is alleged to be practically impenetrable to all known hacking methods and attempts to crack the encryption with available computing power would take years. However, researchers believe that it is only a matter of time before AES can be compromised. According to a recent article in Wired magazine, “quantum computers, which are fundamentally different from traditional computers because they leverage quantum mechanics to do calculations, could easily decrypt the advanced encryption we use widely.” In the meantime, experts have claimed to defeat the security of devices with AES and RSA encrypted data by attacking the device itself and exploiting engineering flaws in them.

The first section of this chapter had multiple intentions. While providing a background on the evolution of encryption, it also showed that in over 2,000 years, only one method, the one-time pad, has been used to encrypt data that could not be cracked given sufficient time. It also showed that even in this one instance in which this encryption method was proven mathematically to be perfectly secret, it could still be exploited in the right circumstances. As this thesis develops, this critical point will be revisited; encrypted data will likely always be vulnerable. This understanding is an essential element of informed debate over the idea that an industry orchestrated option to access encrypted devices and communications should be a requirement. It is the crux of


the argument that technologists embrace as they battle those in favor of exceptional access, and one that has not changed in over 20 years.

C. THE CRYPTO WARS TO PRESENT DAY

As mentioned in the literature review, the debate over encryption that populated headlines over the past two years is not novel. In the time DES was publicly compromised and an AES solution was developed, a significant event relative to encryption unfolded. During the 1990s, those in favor of the government’s exceptional access to encrypted data squared off philosophically against those in favor of technology in a time referred to as the Crypto Wars. The Crypto Wars is an important event worth touching upon as it reveals the embedded positions and rhetoric of two groups that set the foundation for what has become an interminable debate. The flashpoint of the event was over two significant issues, a technology referred to as the Clipper Chip and export controls on encryption technology. Following the Crypto Wars in the late 1990s and early 2000s, the debate was relatively quiet about encryption and the government’s need for exceptional access. In 2013, the illegal release of information by Edward Snowden triggered events within the United States that brought the encryption debate back to a daily conversation topic.

1. The Clipper Chip

The Clipper Chip proposal was an initiative launched under the Clinton administration to address concerns by intelligence and law enforcement agencies over access to encrypted information. The actual chip was a piece of hardware known as MYK-78 that was to be installed in communication devices to enable encryption, while also allowing for government access under set judicial rules. The proposal was outlined by the NIST and approved by the Department of Commerce in the federal information

---

processing standards (FIPS) publication entitled, Escrowed Encryption Standard (EES). According to the White House:

This new technology will help companies protect proprietary information, protect the privacy of personal phone conversations and prevent unauthorized release of data transmitted electronically. At the same time this technology preserves the ability of federal, state and local law enforcement agencies to intercept lawfully the phone conversations of criminals.

This goal was accomplished through the use of “spare keys.” These “spare keys” were more formally known as a “key escrow system,” in which the government maintained each chip’s two-part encryption key. When law enforcement obtained lawful authorization, each part of the two-part key would be released by the NIST and Treasury Department. The algorithm to be used in the encryption, Skipjack, was developed by the National Security Agency (NSA). The NSA set forth two requirements for the use of its technology, which was deemed to be significantly stronger than DES; that the government be involved with device manufacturing in the installation of the chip to ensure authorized use and that it include a backdoor for law enforcement known as the law enforcement access field (LEAF).

The Clipper Chip initiative was immediately met with opposition. In fact, “Nearly all of the comments received from industry and individuals opposed the adoption of the


84 Kehl, Wilson, and Bankston, Doomed to Repeat History?, 5.

85 Kehl, Wilson, and Bankston, 5.

86 Kehl, Wilson, and Bankston, 5.
standard, raising concerns about a variety of issues.”¹⁸⁷ Two predominant arguments voiced at the time are important to the analysis of solutions going forward, privacy, compounded by access and vulnerability, and economics.⁸⁸

Privacy advocates argued that the government’s third-party control of the technology and keys opened up the possibility for unauthorized access. This possibility for unauthorized access was articulated in two forms, by the government should its interests so dictate or by an illicit actor through the natural vulnerability of the technology created with a backdoor.

Economically speaking, arguments were made about an unreasonable cost for the technology and its upkeep, competitiveness of U.S. businesses in foreign markets, and an unfair competitive advantage to the one U.S. business chosen to manufacture the chips.⁹⁰ These points of contention were part of comments made by 22 government organizations, 22 industry organizations, and over 275 individuals during the FIPS review process.⁹⁰

Amidst public outcry in opposition to the Clipper Chip, the initial debate on the issue came to a hard stop in 1994; after additional attempts in the 1990s to implement similar proposals, in 2015, it was officially withdrawn.⁹¹ The initial stop was due to a discovery by Matthew Blaze, a computer scientist at AT&T Bell Laboratories, who discovered, “Rogue applications defeat EES by making use of the cipher without the government back door.”⁹² Although similar efforts were made to implement a Clipper Chip solution to access in the mid to latter part of the 1990s, many overwhelming opposition views and technological obstacles prevented the ideas from ever being viable.

---


⁸⁸ Kehl, Wilson, and Bankston, Doomed to Repeat History?, 5.


An additional limiting factor was drastic changes to encryption controls in the United States.

2. Export Controls of Encryption Items

The other front being simultaneously fought by the administration during this time period of the Crypto Wars focused on export controls. Prior to 1996, Cold War era laws limited the dissemination of sensitive weapons and technologies, including encryption, in an effort to give the United States the upper hand in maintaining its security interests in foreign intelligence.\(^{93}\) Two acts were used explicitly in this regulatory activity. According to the National Research Council, “Authority to regulate imports and exports of products with cryptographic capabilities to and from the United States derive from…The Arms Export Control Act (AECA) of 1949 (intended to regulate munitions) and the Export Administration Act (EAA; intended to regulate so-called dual use products).”\(^{94}\) By treating all encryption products as munitions defined under the United States Munitions List as, “articles, services, and related technical data…designated as defense articles or defense services pursuant to section 38 and 47(7) of the AECA,” dissemination of encryption was effectively regulated by the government.\(^{95}\)

However, as internet technology advanced in the 1980s and 1990s, the laws were found effectively to stifle the economic growth of U.S. companies, while failing to deter equal and greater advances of encryption effectively in other countries.\(^{96}\) According to the* Harvard Business Review*, “The lost business resulting from the export control system costs U.S. companies $9.3 billion a year. But the real price of export controls is almost

---


\(^{95}\) Title 22 U.S.C. §121.1.

certainly much higher. Because of the export control system, the United States is losing vast trade opportunities—in Eastern Europe and the developing world.”

This loss brought pressure from the private sector and the U.S. Congress to influence change by the administration. The Clinton administration recognized the issue, and in 1996, released their regulatory proposal entitled, Achieving Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure. In a statement from the White House, Vice President Al Gore stated, “For export controls purposes, commercial encryption products will no longer be treated as munitions. After consultation with Congress, jurisdiction for commercial encryption controls will be transferred from the State Department to the Commercial Department.” The administration remained focused in this plan on key escrow and key recovery.

Congressional leaders exerted further deregulatory pressure by drafting legislation like Representative Robert Goodlatte’s Security and Freedom through Encryption (SAFE) Act. Responding to the White House plan, Senator Conrad Burns stated, “[T]he third version of the Administration’s Clipper Chip proposal is a swing and a miss. It’s time to quit relying on government mandates for what is truly a matter of great concern to the private sector: the expansion of commerce on the Internet and other computer networks.”

In the face of mounting pressure, in 1999 the administration made further concessions to export control, which resulted in a regulatory rule change by the Department of Commerce. Ultimately, the export administration regulations were amended to remove language about key escrow, allow for the export of encryption items to all destinations with the exception of countries supporting terrorism, and fall in line

---


with many of the stipulations set forth in the Wassenaar Arrangement. In fact, the Wassenaar Arrangement set forth many of the guidelines, elements, and procedures that became the basis for many of the encryption export policies of the United States and the 42 other countries that joined following its establishment in 1995.

With this 1999 announcement and 2000 rule change, the Crypto Wars effectively ended. Those in opposition to government access, privacy advocates, and private enterprise representatives hailed it as a victory. More importantly, it established a strong, tested foundation upon which to wage a battle against exceptional access. Efforts to revisit the issue would not return in full force until Edward Snowden’s unlawful release of national security information.

3. Snowden

In 2013, NSA contractor Edward Snowden illegally shared a voluminous amount of data and information pertaining to NSA programs. Amongst the documents shared with members of the press was evidence of extensive cooperation and information sharing between the government and communications providers. AT&T, for example, was shown to have shared billions of emails and phone records from 2003 to 2013. At the same time, documents revealed the NSA was collecting an extraordinary number of phone records of Verizon customers daily.

Legal collection of information from communications companies has been authorized historically through statutes like the CALEA, the Electronic Communications Privacy Act (ECPA), and the Foreign Intelligence Surveillance Act (FISA). Snowden’s disclosures revealed that much of the information being gathered on U.S. citizens, and

others, may have been due to an extremely liberal interpretation of some of these acts, and potentially with disregard for these laws in some cases. As a result, two things occurred. The public, surprised by the actions of the government, called for stronger encryption of their communications, and private companies answered these calls. The former Director of National Intelligence stated in 2016, “As a result of the Snowden revelations, the onset of commercial encryption has accelerated by seven years.”

Conscious of the existing laws, companies like Apple and Google implemented encryption protocols that were not only comprehensive but also ensured they would satisfy the restrictions within acts like CALEA. For example, CALEA states that a “telecommunications carrier shall not be responsible for decrypting, or ensuring the government’s ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.” Apple meets this requirement with its encryption, which, in part, re-stoked the encryption debate from the 1990s. Apple states in its privacy policy, “And we can’t unlock your device for anyone because you hold the key—your unique password.”

Not being able to unlock a device was the crux of the argument between the government and Apple following the San Bernardino terrorist attacks. The government’s inability to access the phone of one of the terrorists prompted a renewed outcry from many government officials about the need for a solution to exceptional access. The government attempted to challenge Apple’s resistance to assist by issuing an order to the company under the All Writs Act of 1789. The government allegedly wanted Apple to push an authorized update to the terrorist’s phone using the company’s digital certificate of authentication. The update would have enabled the government to attempt a brute force attack of the device to allow an unlimited number of password attempts without interruption. Apple, and others opposed to exceptional access, immediately rejected the


request and challenged it in court. Privacy advocates and technologists echoed the same arguments of the 1990s. They raised concerns that exceptional access solutions would weaken encryption, leave U.S. companies at a disadvantage in the global market, and potentially compromise lawful peoples’ rights to privacy from the government on their electronic devices.

Privacy advocates and technologists are on the prevailing side of the debate, as encryption has proliferated unfettered. The rapid advances in encryption and actions of technology companies caught intelligence and law enforcement agencies off-guard. Law enforcement was already struggling to stay afloat as it faced a growing number of investigations involving digital evidence. The added complications of modern-day encryption have further stymied some of their efforts to fight crime and terrorism.

D. THE CHALLENGE FOR U.S. LAW ENFORCEMENT

While those in opposition to exceptional access have been quietly enjoying what has become the status quo for protecting data, those on the other side of the debate, namely law enforcement, have experienced growing challenges in fulfilling their duties to those they serve and protect. As criminal investigators, law enforcement is tasked with collecting evidence that can be used by the government to prove guilt or establish innocence for a number of incidents that range from car accidents to human trafficking. For any investigation, dozens of pieces of evidence can be integral to achieving their goals, but mobile devices are quickly becoming a universally present evidence source for a responding law enforcement officer.

As society moves towards a greater use of mobile devices, the reliance on them for evidentiary value has become the norm. As a result, digital laboratories in police departments and federal law enforcement agencies are rapidly filling up with digital evidence as devices are seized by law enforcement in the course of investigations. The Law Enforcement Cyber Center, a collaborative project of the International Association of Chiefs of Police (IACP), RAND Corporation, and the Police Executive Research

---

Forum (PERF), funded by the Bureau of Justice Assistance, at the U.S. Department of Justice’s (DOJ) Office of Justice Programs reports that departments around the country face large digital evidence backlogs.108 According to Hitchcock et al., “The issue of the increasing backlog of digital evidence waiting to be examined in many police departments is well documented.”109 A recent media outlet’s investigation into backlogs of electronic evidence reported, “The explosion of smartphones and apps, and the growing size of computer hard drives has created a glut of evidence for investigators in recent years.”110 In Maryland, for example, the state police investigations lab that processes electronic evidence has a 10-month backlog.111 Encryption, in addition to the sheer volume of devices, is a contributing factor to the increased wait times.

The issue is not exclusive to the United States. Although this thesis explores options for domestic solutions to encrypted devices, it is important to recognize that countries overseas are encountering an issue that knows no borders. According to Luc Beirens, superintendent of the Federal Computer Crime Unit (FCCU) in Belgium, “The number of seized computers is a multitude of the number that was seized ten years ago. Every person that we search probably owns a desktop computer, a laptop, an iPad, and a smartphone, and in addition you may see a pile of external hard disks. All those systems need to be investigated.”112 Many of those devices are utilizing encryption, which only adds to the backlog.

The volume of electronic evidence is a growing problem for law enforcement, but of equal or greater concern, is the number of devices that exist in evidence that cannot be

108 Law Enforcement Cyber Center, “Understanding Digital Evidence.”
111 Iacone.
accessed due to encryption. As a result of encryption, comprehensible data residing on a device cannot be accessed unless it is decrypted. According to the FBI,

the government’s inability to access information residing on devices is known as going dark. Law enforcement faces two distinct Going Dark challenges. The first concerns real-time court-ordered interception of data in motion, such as phone calls, e-mail, text messages, and chat sessions. The second challenge concerns “data at rest”—court-ordered access to data stored on devices, like e-mail, text messages, photos, and videos. Both real-time communications and stored data are increasingly difficult for law enforcement to obtain with a court order or warrant. This is eroding law enforcement’s ability to quickly obtain valuable information that may be used to identity and save victims, reveal evidence to convict perpetrators, or exonerate the innocent.113

Forensic Focus, founded in 2002, claims to be the internet’s leading digital forensics portal for computer forensics.114 In a September 2015 survey of 500 digital forensic examiners conducted by the group, they asked, “In your opinion, what is the biggest challenge facing digital forensic investigators today?”115 Approximately 21% of respondents answered that encryption was among the top two concerns of the 12 options; cloud forensics was the largest concern.116

Several law enforcement leaders have been vocal on the issue, most rallying behind former FBI Director James Comey. Director Comey made a spirited charge at the issue in hearings and panels he attended during his tenure.117 This drive was despite the fact that encryption did not initially appear to be the same challenge for federal agencies

113 Federal Bureau of Investigation, “Going Dark.”


116 Scar de Courcier.

as it is for state and local law enforcement officials. In 2016, FBI general counsel Jim Baker said that the FBI is able to get the data it needs 87% of the time. However, in the first six months of fiscal year 2017, the FBI’s ability to access the data it needed on electronic devices dropped to 54% of the time. This drop-off indicates how quickly the encryption problem is growing.

Data presented from local law enforcement supports this belief. The Manhattan District Attorney, Cyrus Vance Jr., stated in testimony on Capitol Hill that “local law enforcement agencies do not have the resources to access each lawfully-seized device.” Vance has been extremely transparent about the issue and has well-articulated the argument in his own interviews and testimony since thrusting New York City’s challenges with encrypted devices into the spotlight in 2016. According to Vance, between 2015 and 2016, the number of Apple devices part of investigations in his office that cannot be cracked, including rape and murder cases, quadrupled to 423. (See Figure 1) In testimony on Capitol Hill to the Senate Armed Services Committee (SASC), he reiterated this sentiment stating:

Let me give you the impact of this new encryption protocol introduced by Apple. In my Office alone, we now have more than 310 lawfully-seized iPhones running iOS 8 or 9 that are completely inaccessible, despite court-ordered search warrants having been issued for them. These devices represent hundreds of real crimes against New Yorkers that we cannot fully investigate, including cases of homicide, child sex abuse, human trafficking, assault, cybercrime, and identity theft.

---


120 United States Senate Committee on Armed Services, *Written Testimony of New York County District Attorney Cyrus R. Vance, Jr.*

121 United States Senate Committee on Armed Services, *Written Testimony of New York County District Attorney Cyrus R. Vance, Jr.*

122 United States Senate Committee on Armed Services, *Written Testimony of New York County District Attorney Cyrus R. Vance, Jr.*
By all appearances, the ability of the Manhattan District Attorney’s Office to utilize device data effectively potentially to prosecute cases with significant community impact is foiled in many instances due to encryption, as shown in Table 1.

Table 1. Encrypted iOS Devices Related to Open Investigations at the Manhattan District Attorney’s Office in 2016

<table>
<thead>
<tr>
<th>Model</th>
<th>Number of Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPads</td>
<td>30</td>
</tr>
<tr>
<td>iPhone 4S</td>
<td>1</td>
</tr>
<tr>
<td>iPhone 5</td>
<td>9</td>
</tr>
<tr>
<td>iPhone 5C</td>
<td>5</td>
</tr>
<tr>
<td>iPhone 5S</td>
<td>51</td>
</tr>
<tr>
<td>iPhone 6</td>
<td>166</td>
</tr>
<tr>
<td>iPhone 6 SE</td>
<td>2</td>
</tr>
<tr>
<td>iPhone 6+</td>
<td>66</td>
</tr>
<tr>
<td>iPhone 6S</td>
<td>63</td>
</tr>
<tr>
<td>iPhone 6S+</td>
<td>30</td>
</tr>
<tr>
<td><strong>Total Devices</strong></td>
<td><strong>423</strong></td>
</tr>
</tbody>
</table>

In an interview with *Fortune* magazine, Vance speculated that based on the numbers of encrypted, inaccessible cell phones in New York County, and approximately 20,000 counties in the United States, thousands of mobile phones could be in the hands of investigators and prosecutors that are of little use due to encryption. In his testimony to the SASC, he corroborated this claim with information from other police departments across the country. District Attorney Vance stated:

The data from across the country tells a similar story. In California, the Los Angeles County Sheriff’s Department has amassed more than 150 inaccessible devices, the Los Angeles Police Department has more than 300, and the Roseville Police Department has more than 200. Riverside County, California has 12 inaccessible devices connected to murder cases alone. The Charlotte-Mecklenburg Police Department in North Carolina has 160 inaccessible devices. In Texas, the Harris County District Attorney’s Office collected more than 100 inaccessible devices in 2015.

---

124 Roberts.
and have encountered 8 to 10 inaccessible devices per month so far this year. And in Massachusetts, the Suffolk County District Attorney’s Office has 129 inaccessible devices.\textsuperscript{125}

The encrypted devices presented in this testimony, from a small fraction of the local law enforcement agencies in the country, are the overwhelming challenge law enforcement faces.

District Attorney Vance’s presence on the Hill, along with former Director Comey’s, had the intention of spurring action on the part of federal legislators. Their efforts appear to have fallen short, as no momentum could be gained to move legislation forward. Senators Diane Feinstein and Richard Burr of the U.S. Senate Select Committee on Intelligence floated the idea of legislation with a discussion draft entitled, \textit{Compliance with Court Orders Act of 2016}.\textsuperscript{126} It was met with the same level of resistance as proposals during the Crypto Wars, lacked support from the Obama Administration, as well as the House of Representatives, and was ultimately never filed.\textsuperscript{127} Senator Mark Warner and House of Representatives Chairman Michael McCaul did file bicameral legislation in the 114th Congress. Their \textit{Digital Security Commission Act of 2016} would have established a commission of, “the most capable experts and stakeholders from law enforcement, the technology industry, the intelligence community, and privacy and civil liberties communities to discuss the challenges and advise policy makers on this complex issue [of encryption].”\textsuperscript{128} The ultimate goal would have been to provide recommendations on the subject, upon which lawmakers could act. However, following

\begin{itemize}
\item \textsuperscript{125} United States Senate Committee on Armed Services, \textit{Written Testimony of New York County District Attorney Cyrus R. Vance, Jr.}
\end{itemize}
its introduction to the House, this bill never left the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.129

Despite the calls from law enforcement in 2016, no other legislation was filed to assist the government with access to encrypted devices; likewise, nothing of substance appears to be on the horizon during the 115th Congress. Thus far, Congress has proven unable to legislate a solution to the device encryption issue; if it has shown anything over the past 20 years on the issue, it is reticence. This stance does not change the data conveyed by District Attorney Vance about the growing numbers of inaccessible encrypted devices that are stacking up in law enforcement evidence rooms.

As this chapter has discussed, the Crypto Wars of the 1990s ended with the government surrendering efforts to gain exceptional access to the interests of personal privacy and global commercial competitiveness. Since then, governmental needs to access encrypted evidence, especially on devices, has grown exponentially. In the United States, solutions to bridging this growing divide have proven elusive. Given the lack of legislative progress and enduring arguments from the Crypto Wars of the 1990s, an examination of encryption policy in other countries, in an effort to address the issue in the United States, is in order.

III. ENCRYPTION POLICY IN ISRAEL

The Israeli encryption control mechanisms operate without directly legislating any form of encryption-key depositories, built-in back or front door access points, or other similar requirements. Instead, Israel’s system emphasizes smooth initial licensing processes and cultivates government-private sector collaboration.130

—Attorneys Matthew Waxman and Doron Hindin

These people [from the Israel Police’s cybercrime unit] can take almost any hardware product and extract information from it. Even if it had been dropped into water, burnt, probed or smashed. If there is a physical way to extract information from it, the cybercrime unit laboratory will be able to do it.131

—Writer Ami Rojkes Dombe

Israel is considered a world leader in cyber and has an established approach to dealing with device encryption.132 Israel’s sociocultural security environment is the foundation of its approach. The country’s location in the Middle East and its policies on military service has forged a mindset of security and a strong network amongst its inhabitants. The structural feature in its approach is the law enforcement unit tasked with device encryption. The cybercrime unit consists of a centralized forensic unit and a network of officers strategically located across the country under unified control who specialize in data extraction from electronic devices. The unit’s work is enhanced by the relationships the government has with the military, private sector, and academia. Finally, a regulatory framework and applicable laws exists that provide context to its approach.

130 Waxman and Hindin, “How Does Israel Regulate Encryption.”
The result is a country that appears to have a reasonable approach to the extraction of data from encrypted devices without leaving the country mired in a debate over exceptional access.

A. THE SOCIOCULTURAL ENVIRONMENT OF ISRAEL

The State of Israel, declared on May 14, 1948, is a country of approximately 8.1 million people, 75% of whom are ethnically Jewish.\textsuperscript{133} Israel’s government is a parliamentary democracy that came, “into existence with surprisingly robust and tested democratic institutions and traditions.”\textsuperscript{134} In part, due to its location, Israel has endured a tenuous security status for almost all of its existence. The country has engaged in wars with Arab forces on no less than five occasions in 1948–1949, 1956, 1967, 1973, and 1982.\textsuperscript{135}

In regards to a sociocultural mindset of security, these military engagements served to focus the country and its population on the importance of security and resilience under values of nationalism. Military service for both sexes is compulsory at the age of 18 for the majority of the population, Jews, and Druze, with 32 months required for enlisted men and 24 months for enlisted women.\textsuperscript{136} This requirement was intended to be more than a call to arms.\textsuperscript{137} Bringing the nation closer together, while instilling a military focus based on a shared experience, ensures that the majority of citizens, including those in government, recognize the need for policies and relationships to preserve security. Further, with the government recruiting for certain positions beginning in high school, it cultivates security knowledge at a young age and lasting relationships beyond military service.\textsuperscript{138} The result is Israel’s security network, an integrated relationship between


\textsuperscript{136} Central Intelligence Agency, “The World Factbook, Middle East: Israel.”

\textsuperscript{137} Morag, Comparative Homeland Security, loc. 4529–4531 of 8910.

\textsuperscript{138} Cyber Supremacy/Japan Rising.
security and civilian actors that shapes the country’s policymaking processes and policies in multiple spheres.\textsuperscript{139} Cyber is the relevant sphere in the Israeli network for the purposes of this chapter.

Relative to fostering development in the area of technology, it should be acknowledged that Israel is a world leader in cybersecurity. In 2010, Israel launched the National Cyber Initiative, with the goal of being one of the top five cyber powers in the world by 2015.\textsuperscript{140} Prime Minister Netanyahu refocused this goal on cybersecurity, and in 2017, he declared it had been achieved, with Israel receiving 1/5 of the world’s global private investment in cybersecurity.\textsuperscript{141} Researchers found, “companies in Israel, a country comprising less than 0.11% of the world’s population, are estimated to have sold 10% ($6 billion out of $60 billion) of global encryption and cyber technologies for 2014.”\textsuperscript{142} Israel’s focus on cyber stems from work within the Ministry of Defense (MOD), and a coordinated effort on the part of its government, to compensate for a lack of other resources and to pre-empt further costly wars with its neighbors. A 2012 study conducted by McAfee and the Brussels think-tank, Security and Defence Agenda, found Israel to rank at the top of 23 countries in cyberdefense.\textsuperscript{143}

This growth in Israel’s private cybersecurity industry reflects the integrated relationship between its security and civilian sectors. As Israeli defense journalist Alon Bed-David observes, “The whole of the Israeli cyber industry relies on knowledge gathered by people serving in Israel’s different security agencies and military.”\textsuperscript{144} Cyber intelligence units presently make up the largest populated units of the Israeli Defense Force (IDF).\textsuperscript{145} Approximately 20,000 cyber-soldiers are in the IDF and the country is

\begin{flushleft}

\textsuperscript{140} Benoliel, “Towards a Cybersecurity Policy Model.”

\textsuperscript{141} Cyber Supremacy/Japan Rising.

\textsuperscript{142} Waxman and Hindin. “How Does Israel Regulate Encryption.”

\textsuperscript{143} Benoliel, “Towards a Cybersecurity Policy Model.”

\textsuperscript{144} Cyber Supremacy/Japan Rising.

\textsuperscript{145} Cyber Supremacy/Japan Rising.
\end{flushleft}
constructing the Beersheeba cybersecurity complex to centralize their efforts. The complex that will house these cyber-soldiers, located in Israel’s fourth largest city, is a $5B compound dedicated to defensive and offensive cyber operations, and will arguably be the largest infrastructure project in Israel’s history.146

The result of this emphasis on cybersecurity in the military is that the IDF has become the largest human resources organization for the country’s cybersecurity industry. The skills and methods learned by these young soldiers, who are typically free of conscription by the age of 23, are priceless in the open market. The training and missions undertaken in the IDF’s C4I Directorate, and specifically the IDF’s elite cyber group, Unit 8200, are unsurpassed by almost any country other than the United States.147

One assignment for personnel of Unit 8200 was documented as follows:

Break into the computers of a country that remained in a state of hostility with Israel. The task contained several hurdles: First, figure out how to get into those computers; second, how to crack the encryption; and finally, the monumental challenge, how to access the “enormous amount” of computing power necessary to decrypt the data.148

One of the IDF members tasked with this assignment went on to start the successful web development company Wix.149 Israel has former soldiers founding and staffing similar technology companies like Waze and Indegy, and most importantly for this thesis, the NSO Group, White-Hat Ltd., and Cellebrite.

For example, White-Hat Ltd., an Israeli company founded by a former IDF soldier, delivers cyber-intelligence services around the world and is staffed with a large


147 The C4I Directorate is a support corps of the IDF responsible for computers and communications. Unit 8200 is an elite unit within the C4I Directorate and is responsible for signal intelligence and code decryption.


149 Behar.
number of former IDF cyber-soldiers.\textsuperscript{150} During the WannaCry cyber-attack in 2017, White-Hat Ltd. sent its customers, many of whom are Israeli based, a “vaccine,” within an hour of the attack.\textsuperscript{151} Meanwhile, Israel’s top cybersecurity official, Baruch Carmeli, reported no evidence indicating the country fell victim to this attack.\textsuperscript{152}

Similarly, Cellebrite Mobile Synchronization, Ltd., founded in Israel in 1999, “develops solutions for the mobile retail and forensic industries...[and] offers a universal forensic extraction device (UFED)...[for] law enforcement, military, intelligence, security, and government agencies in Israel and internationally.”\textsuperscript{153} Cellebrite employs IDF Unit 8200 veterans including Gilad Sahar and Tom Gol, who later left to establish a counter-UAV company.\textsuperscript{154} A highlight video of the Israel Police cybercrime unit situation room in Israel features a technician using a Cellebrite UFED instrument, which is used to extract data from devices.\textsuperscript{155} Cellebrite also operates a subsidiary, Cellebrite USA Corp., that contracts services for U.S. law enforcement agencies including the FBI, Secret Service, Customs and Border Patrol, Immigration and Customs Enforcement, Drug Enforcement Administration, and Securities and Exchange Commission.\textsuperscript{156}

\begin{itemize}
\item \textsuperscript{152}Solomon.
\end{itemize}
Contracts with these agencies are part of the approximately 60,000 contracts the company has in over 150 countries.\textsuperscript{157}

As these examples show, the cybersecurity talent and skills cultivated in Israel’s sociocultural security environment are evident. The country’s cyberdefenses rank at the top among developed countries. Personnel contributing to this achievement in the military have gone on to establish or be part of Israeli companies that excel in the field. This expertise is the basis for Israel’s efforts relative to data extraction from encrypted devices undertaken by its police force. The Israel Police exhibit its own abilities, supported by this expertise, through its cybercrime unit.

B. STRUCTURAL DIMENSIONS TO ENCRYPTED DATA EXTRACTION

The Israeli government has a centralized national police force, the Israel Police, under the control of the state government, with districts throughout the country.\textsuperscript{158} The country benefits by organizing a singular effort to defeat device encryption for law enforcement purposes. A notable feature of the police force is that all Israel Police officers have already served in the IDF. According to the Israel Police website, all potential police officer candidates must possess an IDF certificate of discharge, further affirmation of the Israeli security network that exists within the country.\textsuperscript{159} Within this police force of former IDF soldiers is a unit dedicated to cybercrime, including the extraction of data from encrypted devices.

1. Israel Police Cybercrime Unit

Within the Israel Police force, a centralized cybercrime unit operating under LAHAV 433 has been in existence for approximately three years, although it dates back


to the 1990s as a less formal organization. This cybercrime unit possesses a forensic capability, and under the unit, is a network of cyber officers throughout Israel serving individual communities that have the ability to elevate complex tasks to their headquarters. Much of the unit’s time is spent on the forensic extraction of data from computers and devices, especially in the individual districts of the police force. According to a 2017 report from the Israel State Comptroller:

The District Command directs the cyber officers to assist other investigative teams in the district in handling evidence captured by digital devices such as a computer, tablet, smartphone, and camera...The State Comptroller’s Office found that the vast majority of cyber officers’ work in the provinces focuses on producing digital evidence.

In some cases, this outcome is to the detriment of other cybercrime investigations. The report details an excess of attention directed towards digital evidence extraction, at the cost of focusing efforts on complex cybercrime cases. Despite the criticism the unit received relative to complex cases, it appears to be accomplished in its ability to extract data from devices. According to one Israeli government publication:

The third pillar of the cybercrime unit is the forensics laboratory. These people can take almost any hardware product and extract information from it. Even if it had been dropped into water, burnt, probed or smashed. If there is a physical way to extract information from it, the cybercrime unit laboratory will be able to do it. Hard disk drives, cellular phones, portable storage devices and many other types of media.

As mentioned in the previous section, the Israel Police use technology developed by Cellebrite for data extraction, which is similar to some U.S. law enforcement organizations that also depend on Cellebrite.

---

160 LAHAV 433 is a comparable organization to the United States Federal Bureau of Investigation, although it still falls under the Israel Police. See Dombe, “Cybernetic Investigations.”


163 Dombe, “Cybernetic Investigations.”
The Israeli modus operandi for cybercrime is distinct from that of the United States, which relies on a decentralized system of multiple federal agencies, along with state and local agencies often acting independently to combat challenges like device encryption. On an operational level, some U.S. law enforcement agencies have forensic laboratories or access to state laboratories but throughout the country lack the robust, unified approach Israel uses. Attempts to address this deficiency with programs like the FBI’s regional computer forensic laboratories (RCFLs) or the Secret Service’s electronic crimes task forces (ECTFs) have not yet succeeded in meeting the needs of the United States in this area.

2. Partnerships

The Israeli cybercrime unit’s work is enhanced by the relationships the government has to the military, private sector, and academia. These partnerships contribute to the structure and approach of the unit to encryption.

First is recruitment for the Israel Police from the military. All police officers are former members of the IDF. No documentation is available stating that recruits joining the Israel Police were trained in cyber in the military, or that those who were are being directly funneled to the cybercrime unit. However, the Israel Police rely on military veterans in the laboratory of its cybercrime unit. In this way, some level of military training is leveraged for the purposes of device encryption.

Second, relative to private sector relationships, companies like Cellebrite that also recruit from the military, are a source for equipment to Israeli law enforcement for device encryption extraction. Further, Israel has pushed to improve the relationships between the private sector and law enforcement through events like, “hackathons.” In 2015, Ben-Gurion University of the Negev, in coordination with LAHAV 433, held a “Future Cop”

---

164 Israel Police, “Recruitment Screening Process.”
165 Ahronheim, “How Israel Is Thinking outside the Box to Stop Terror.”
hackathon amongst police, private security operators, civilians, and students to solve hi-
tech problems facing law enforcement.\textsuperscript{166}

The hackathon referenced previously also represents collaboration with academia. Ben-Gurion University of the Negev (BGU) was one of the first two schools of higher education to partner with the government; the other was the University of Tel Aviv.\textsuperscript{167} BGU is also located at the site where the military is constructing its new $5B facility. Part of the facility already constructed is the BGU cyber security research center. The center is a partnership between the government and the university, which houses a number of labs, one of which is dedicated to device issues like encryption in the mobile security lab.\textsuperscript{168}

The Israel Police’s method of extracting encrypted data from devices described previously happens through its cybercrime unit. This method is not altogether different from law enforcement’s approach in the United States, except that in Israel, it is under one umbrella and is not lobbying to change its approach. The relationships established in Israel with the military, private sector, and academia enhances the country’s ability to exploit encrypted data on devices. Techniques used by the police force or private companies to obtain this information would be considered a form of ethical or lawful hacking.\textsuperscript{169} The term is a diplomatic phrase to describe law enforcement’s legal exploitation of encrypted data on a device. This course of action is one that has, thus far, been advocated for by the Israeli security network and acted upon by the Israel Police.

The extraction of encrypted data in Israel appears to occur without the prevalence of debate experienced in the United States. The use of lawful hacking as an alternative to


\textsuperscript{167} Benoliel, “Towards a Cybersecurity Policy Model.”


\textsuperscript{169} Lawful hacking is a term broached by Susan Hennessy and other cyber scholars as an alternative to compelling access. See Hennessy, “Lawful Hacking and the Case for a Strategic Approach to ‘Going Dark’”; Bellovin et al., “Lawful Hacking,” 1–63.
legislating exceptional access may partly be the reason why Israel has escaped such a paralyzing debate.

C. ENCRYPTION REGULATORY POLICY AND APPLICABLE LAWS IN ISRAEL

The final aspects of Israel’s encryption approach are the regulatory frameworks within which the Israel Police must act. To cover device encryption policy in Israel and its potential applicability to the United States properly, this section examines Israel’s regulatory policy and applicable laws.

1. Regulation of Encryption

Some have speculated that the Israeli encryption laws, along with the cultural norms of the country, allow for superior technological development.\textsuperscript{170} One scholar on Israel states, “This approach is, in fact, quite characteristic of Israel, in that flexibility and ad hoc solutions are generally preferred to more rigid and formalistic approaches.”\textsuperscript{171} This approach fosters the capabilities of Israeli technology companies to develop while enhancing the relationships of the government.

Many countries control the production, sale, and export of encryption technology through dual use regulations. Dual use goods and technologies refer to those things that are typically used for civilian purposes but may have military applications. The Wassenaar Arrangement influences the United States’ position on dual use regulations including encryption export policies. Encryption-capable products are covered under this arrangement; Israel is not a member. Instead, Israel relies on a number of laws and regulations passed within the country over the past 60 years. Israel controls encryption and other products primarily through its Law Governing the Control of Commodities and Services Law—1957 (5717), Order Regarding the Engagement with Encryption Items—

\textsuperscript{170} Waxman and Hindin, “How Does Israel Regulate Encryption.”
\textsuperscript{171} Morag, \textit{Comparative Homeland Security}, loc. 1493–1494 of 8910.
1974 (5734), and a 1998 amendment to the 1957 law, the Commercial Encryption Items Export Controls Policy, that was updated in 1999.\textsuperscript{172}

In 2014, Israel sold 10\% of global encryption.\textsuperscript{173} The Government of Israel explains that the regulatory actions it takes are partly responsible. The Israel Ministry of Defense states on its website:

In applying the system of control and licensing of encryption items, every effort is made to maintain a proper balance between the needs of the individual and the industry whilst keeping the essential requirement of the State to maintain adequate control over the dissemination of means of encryption in Israel and abroad. The purpose of regulating engagement in items of encryption is to enable the Israeli encryption industry—one of the most advanced in the world—to develop, produce, sell and export its products while at the same time safeguarding the national security interests of the State of Israel.\textsuperscript{174}

Israel’s stated intention is achieved through longstanding regulatory practices pertaining to encryption that are unique to the country.

Generally speaking, policy breaks down into the following areas: use, development and production, import for sales and distribution purposes, sales within Israel, and export.\textsuperscript{175} Each area is subject to licensing requirements, typically under a license for engagement in encryption items, under which Israel regulates the technology. In almost all cases, to engage with encryption, the government must be made aware, assess the technical aspects of the product, and issue a license.\textsuperscript{176} The few exemptions that exist typically apply to electronic signatures and open-source encryption downloadable from the internet.\textsuperscript{177} Ultimately, one of four different types of licenses is issued following approval: restricted licenses, special license, general license, or free

\begin{itemize}
  \item \textsuperscript{173}Waxman and Hindin, “How Does Israel Regulate Encryption.”
  \item \textsuperscript{174}Israel Ministry of Defense, “Encryption Controls in Israel.”
  \item \textsuperscript{175}Israel Ministry of Defense.
  \item \textsuperscript{176}Israel Ministry of Defense.
  \item \textsuperscript{177}Israel Ministry of Defense.
\end{itemize}
means license.\textsuperscript{178} The restricted license and special license have the most stringent requirements, including annual renewal, and are characteristically issued to those engaging with restricted countries or sectors.\textsuperscript{179}

Two important points can be made about the majority of licensing that benefits the country. The first is the simplicity and speed of the process. The government’s website lays out instructions for emailing or mailing the application and technological specifications of the encryption to the Encryption Control Unit of the Defense Export Control Agency.\textsuperscript{180} According to the MOD, the average time for the licensing process in 2014 was just under eight days.\textsuperscript{181} The second point concerns the benefits that accompanied the addition of the Free Means License in 1998, under the amendment previously referenced. It literally means that encryption items can be declared “decontrolled,” or free, following receipt and approval of the application, which then renders them exempt from further controls.\textsuperscript{182} A list is published on the Government of Israel’s website. Over 11,500 licenses have been issued since 1999.\textsuperscript{183} Most commercial vendors, including Apple for their IOS and Google for their Android operating systems, fall into this category.\textsuperscript{184}

It is important to note that:

The Israeli encryption control mechanisms operate without directly legislating any form of encryption-key depositories, built-in back or front door access points, or other similar requirements. Instead, Israel’s system emphasizes smooth initial licensing processes and cultivates government-private sector collaboration.\textsuperscript{185}

\begin{flushright}
\textsuperscript{178} Israel Ministry of Defense.\\ 
\textsuperscript{179} Israel Ministry of Defense.\\ 
\textsuperscript{180} Israel Ministry of Defense.\\ 
\textsuperscript{181} Israel Ministry of Defense.\\ 
\textsuperscript{182} Israel Ministry of Defense; Waxman and Hindin, “How Does Israel Regulate Encryption.”\\ 
\textsuperscript{184} Israel Ministry of Defense.\\ 
\textsuperscript{185} Waxman and Hindin, “How Does Israel Regulate Encryption.”
\end{flushright}
Scholars argue that the characteristics of this user-friendly regulatory process encourage participation, innovation, and freedom in the field of encryption. This efficient, simple regulatory process establishes a foundation for partnerships between the government and the private sector discussed in the previous section. In addition, the processes allow the government to have insight into novel encryption technologies before they hit the market and better position themselves to manage issues effectively with them down the road with this advance knowledge. Some of these claims are speculative and evidence is lacking to prove causality. However, policies of the country have clearly launched it into a category of top producers of encryption while allowing it to also be a world leader in cybersecurity.

2. Civil Liberties and Stored Information in Israel

The laws protecting information stored on devices in Israel are comparable to those in the United States under the Fourth Amendment of the U.S. Constitution. The basis for them can be found in the protection of civil liberties, where one independent watchdog ranks the two countries similarly in the countries’ observance of the rule of law. Looking at civil liberties as a whole, the United States ranks higher than Israel, and although security is a cited factor, it is not clear that a subcategory of cybersecurity is the reason for the disparity.

In Israel, since the First Knesset was unable to put a constitution together, it legislated basic laws on various subjects. In March 17, 1992, it passed the Tenth Basic Law of Israel, Human Dignity and Liberty. The purpose of the law is to “protect human dignity and liberty, in order to establish in a Basic Law the values of the State of Israel as

---

186 Waxman and Hindin.”


a Jewish and democratic state.”

This basic law has several subsections, and all encompass the spirit of the title.

The portions of the basic law relevant to searching a device can be found in sections three and seven, which set forth the protection of property and rights to privacy, respectively. Section three states, “There shall be no violation of the property of a person.”

The relevant subsections of section seven read, “(a) All persons have the right to privacy and to intimacy... (c) No search shall be conducted on the private premises of a person, nor in the body or personal effects... (d) There shall be no violation of the confidentiality of conversation, or the writings or records of a person.”

It is important to note that the final section of this law does lay out circumstances in which a state of emergency is declared, which can allow the government to, “deny or restrict rights,” under this law for a reasonable amount of time. Absent the state of emergency, the government is required to follow legal procedures and obtain a warrant from a court to search a device. The legal standard to obtain a warrant in Israel, like the United States, is based on reasonableness. An Israeli court may issue a search warrant if the judge, “has reason to believe that it was used or is intended to be used for an illegal purpose.”

D. CONCLUDING THOUGHTS

In research for this thesis, the only reference to the encryption debate emanating from Israel was a comment regarding end-to-end encryption service by Israeli Intelligence Minister Yisrael Katz. Katz stated in a conference, “We will not block these

---


190 Israel Knesset.

191 Israel Knesset.

192 Israel Knesset.


services [like WhatsApp].” Further, no documented debates have taken place in the Knesset or comments made from Prime Minister Netanyahu expressing concern or consternation over the issue. Meanwhile, officials from countries like the United States, Canada, Brazil, Spain, the United Kingdom, France, Belgium, and Australia all offer opinions and concerned debate on exceptional access. All other references relative to Israel concerning exceptional access pertained to Israel’s Cellebrite, as the reported means by which the FBI was able to access the phone of the San Bernardino terrorist.

The question of whether Israel’s ability to access encrypted devices is better than the United States is a matter of debate; with a lack of publicly available information on the subject, this thesis is unable to make such a determination. Instead, it affirms several other points germane to the debate that indicate this aspect of Israel’s approach is worthy of consideration.

The country of Israel relies on its centralized law enforcement and cybercrime unit with assistance from private partners like Cellebrite, along with ties to the military and academia. Research reveals that Israel is accepting of its approach to the present-day issue of device encryption. This acceptance of its resilient security-minded approach is likely a product of the country’s shared military service and excellence in the field of cyber. No concerns or controversies are voiced about exceptional access by the prime minister, members of the Knesset, or other political leaders in the country. The population, a significant number of whom are involved in burgeoning high technology fields, remains silent on the methods used by the Israel Police and the subject of exceptional access at large.

No indication can be seen that technology companies like Apple have any obligations placed on them to assist with exceptional access; nor have companies publicly articulated complaints if such demands were made of them. Quite the opposite; Apple has invested over $1.2B in Israel, and opened a research and development center in Herzliya,

where it employs over 800 local hardware and software engineers on its emerging products.\textsuperscript{197} Scholars have indicated that Israel’s streamlined regulatory framework may be a factor in the assistance it receives from the private sector.\textsuperscript{198} No evidence has been found to support such a claim, but it is not an unreasonable assumption.

Israel received high rankings in categories used to assess the level of freedom in the country, and the country’s government is recognized as being protective of its citizens’ civil liberties.\textsuperscript{199} In an illustration of the Israeli judiciary’s stance on device privacy and protection of its citizens’ rights, in June 2017, the Israeli Supreme Court ruled that a warrant is necessary to search a device even when consent is given by the owner.\textsuperscript{200} This standard is much higher than that even seen in the United States, where only consent is necessary. When pressed by Israel’s attorney general on the issue, the court replied that the attorney general should seek a legislative change to the law if he believed it was an issue.\textsuperscript{201}

Even in the face of the Israel Supreme Court challenge, no indication can be seen that Israel intends to change its present course on its encryption approach. It stands to reason that concerns, debates, or attempts to change laws in Israel relative to exceptional access have not occurred because the government is comfortable with the position in which it finds itself. The Israel Police’s cybercrime unit has adequate solutions to encryption: an established approach, which harnesses the expertise of the centralized forensic unit, supported by a network of officers across the country, and strong partnerships to bolster their efforts. These solutions are accepted by its populous and persevere because the approach is consistent with the country’s sociocultural mindset of security and resilience.


\textsuperscript{198} Waxman and Hindin, “How Does Israel Regulate Encryption.”

\textsuperscript{199} Freedom House, “Freedom in the World 2017, Israel.”


\textsuperscript{201} Cohen.
IV. ENCRYPTION POLICY IN THE PEOPLE’S REPUBLIC OF CHINA

Article 18: Telecommunications operators and Internet service providers shall provide technical interfaces, decryption and other technical support assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities in accordance with law.  

—China’s Counter-Terrorism Law (2015)

The People’s Republic of China (China), like Israel, has moved on from the debate over exceptional access to encrypted data on devices. As discussed in the last chapter, Israel’s approach is a product of its sociocultural security environment and it relies on the resources and skills of its cybercrime unit and strategic partnerships in the country. This chapter explores and analyzes China’s approach to encryption. China’s cyber forensic efforts are nascent and its approach is more reliant upon regulation and a legal framework to compel exceptional access. Digital evidence was not formally accepted as legal evidence in China until 2012. For those instances in which the government needs access to encrypted data on a device, China’s regulations and laws, and specifically its 2015 counter-terrorism law, has put companies in a position where they are required to provide assistance in extracting data from devices when requested. Like Israel, China has its own cybersecurity partnerships and a centralized forensic effort. However, based on China’s decision to pass the 2015 counter-terrorism law on the issue, those efforts would appear to be secondary to compulsion. In addition, it is important to note that China also has a government with a questionable human rights record preceding

---


203 The focus of this thesis on the People’s Republic of China will be on Mainland China and does not include Hong Kong or Macau.

and during judicial proceedings. This topic is discussed briefly within this chapter, as it provides some context and questions to its law enforcement efforts.

A. THE POLITICAL DESIGN OF THE CHINESE GOVERNMENT AND ITS IMPACT ON ENCRYPTION

The government organs of China consist of the National People’s Congress (NPC), the President, the State Council, the Central Military Commission, the Supreme People’s Court, the Supreme People’s Procuratorates, and local level governments and courts. The government is legally empowered by the country’s constitution. The Constitution of China was adopted on December 4, 1982, and has had some amendments since that time. The constitution gives noteworthy support to China’s ruling party, the Chinese Communist Party (CCP). The CCP came to power in 1949 and has 73 million members, which makes it the biggest political party in the world. The party exerts influence over the government through its political bureau, the Politburo, with most decisions being made or approved by a smaller group within the organization, the Politburo Standing Committee. Their status in the country, and the legitimacy afforded to them by the constitution, give them the ability to control the people and policies of China tightly. The focus of this control is on propping up the CCP and is reflected heavily in the constitution.

Perusing the Constitution of China, within the preamble and its first articles, the ideals and priorities of the country are evident. In the initial preamble of the constitution, the framers state, “the Communist Party of China…ultimately, in 1949, overthrew the rule of imperialism, feudalism and bureaucrat capitalism, won the great victory of the new-democratic revolution and founded the People’s Republic of China.” The constitution opens its statutory articles with, “The People’s Republic of China is a

---


208 National People’s Congress of the People’s Republic of China, “Constitution.”
socialist state...The socialist system is the basic system of the People’s Republic of China. Sabotage of the socialist system by any organization or individual is prohibited.”209 Leading the chief set of laws of China, it is clear that that the interests of the party are of preeminent consideration. This focus on the party is in stark contrast to many countries in the world, including Israel and the United States, which put the rights of their citizens before government power. This distinction is important to recognize, since many activities that would otherwise be considered criminal, or even civilly disobedient, could be interpreted instead as terrorist in nature if the aim of the activity was perceived to undermine the CCP. It was not until 2004 that an amendment added language to the constitution recognizing, “the State protects and preserves human rights.”210 Even with this amendment, widespread reports of repression of political dissent and religious freedom are still common, as well as abuses of human rights. Reports and investigations on the issue focus on law enforcement, which is ultimately the group responsible for the forensic extraction of encrypted data in the country.

B. STRUCTURAL DIMENSIONS TO ENCRYPTED DATA EXTRACTION

The law enforcement apparatus in China is drawn from two organs, the Ministry of Public Security (MPS) and Ministry of State Security (MSS). Police efforts in China are centralized, like Israel, and unlike the decentralized nature of law enforcement organizations in the United States. The MPS falls under the State Council and is tasked with maintaining the country’s domestic public security, comparable to the work of the many law enforcement organizations of the United States. The public security role includes investigating and deterring criminal and terrorist activities. It is vertically structured along with its subordinate organizations as follows in Figure 1.

209 National People’s Congress of the People’s Republic of China, “Constitution.”
210 National People’s Congress of the People’s Republic of China.
1. Forensic Units

The MPS itself consists of 13 bureaus and several support entities, including three research institutes. Part of MPS’s domestic responsibilities is forensic device data extraction and is the centralized agency overseeing the task. “[In 2000] the MPS established the Public Information Network Security Supervision Bureau to deal with cybercrime investigation, during which a department responsible for computer forensic examination was established in the college of MPS.”

The acceptance of digital evidence in judicial proceedings is relatively new, with official initiation in courts in March 2012. Device data extraction is also handled in the police bureaus at the provincial level, which have the responsibility of, “conduct[ing] forensic/criminalistics analysis of the evidence submitted by the local police stations.” This construct is similar to the description of the structure of forensic efforts in Israel.

---


213 Chow et al., 51.

214 Ebbe, *Comparative and International Criminal Justice Systems*, 175.
2. **Partnerships**

The MPS relies on its private sector for assistance with device data extraction. The private and public sector relationships appear to support the priority of the government in advancing the goals of the CCP, along with traces to relationships forged in military service. As previously discussed, China’s constitution lays out the priorities of the country and focuses on sustaining the CCP. Relative to the connection with military service, like in Israel, it is compulsory. Article 55 of the constitution states, “It is the honourable duty of citizens of the People’s Republic of China to perform military service and join the militia in accordance with the law.” When Chinese citizens turn 18 years old, they are obligated to 24 months of service.

On the forensic cybersecurity side, research indicates the MPS works predominantly with one particular Chinese cybersecurity company, Meiya Pico. Meiya Pico claims to be, “the leading digital forensics and information security products and service provider in China, and dominates 45% digital forensic market share [in the country].” Publications document the relationship, and photographs within those publications show MPS officials using Meiya Pico products. The forensic capabilities of Meiya Pico to extract encrypted data from devices are not as prolific or sophisticated as those of Cellebrite, at least in the Android operating system environment. According to one study, “Cellebrite is the first company in the mobile forensic industry to develop its unique solution for Android devices. Cellebrite’s physical extraction method can bypass

---

more than 200 locks of any types for Android devices.” More than 200 locks of any types for Android devices.”

Meiya Pico claims to have advanced capabilities on its own website but data to support this ability is lacking. Additional relationships to other cybersecurity firms for the purposes of data extraction may exist but do not appear to be as prominent as the one with Meiya Pico. Deputy Minister of Public Security of China. Meng Hongwei spoke to strengthening the public and private sector relationships worldwide in a 2017 speech during an INTERPOL conference. During the conference, he spoke to facilitating information sharing between the sectors in areas of prevention, response, and assistance. The Deputy Minister’s statement is in line with the relationship that already exists between the government and Huawei, a leading Chinese-based mobile device manufacturer. In June and July 2017, Huawei surpassed Apple in global smartphone sales and only trailed Samsung in market shares. Huawei already has partnerships with the MPS, which supports its Public Security Traffic Management Science Institute. In 2011, one U.S. report highlighted Chinese government payments in excess of $228 million to Huawei for research and development. Furthermore, Ref Zhengfei, the founder and CEO of Huawei, was a member of the People’s Liberation Army, where he was a military engineer. Huawei Board Chairwoman Sun Yufang previously worked for the Ministry of State Security. In fact, the U.S. Department of Commerce blocked a Huawei bid for a national

---


220 Meiya Pico, “About Us.”


226 Gertz, “Chinese Telecom Firm Tied to Spy Ministry.”
emergency wireless project in the United States due to concerns about the relationship the company has with the Chinese government.227

These relationships extend beyond Chinese-based companies. Even Cisco, a U.S.-based technology company, has been party to a lawsuit in a U.S. District Court in which it was accused of, “willingly and knowingly provid[ing] Chinese officials with technology and training to access private internet communications, identify anonymous web log (“blog”) authors, prevent the broadcast and dissemination of peaceful speech.”228 After the lawsuit was filed in the United States, one of the named plaintiffs was detained and interrogated by the Ministry of Public Security.229

The relationships the Chinese government has with the private sector appear to have a strong foundation based in a relationship structure designed by the government. However, despite these relationships and the capabilities of MPS and some of the forensic capabilities of companies like Meiya Pico, the government appears to have been more in favor of legislating compliance than overcoming technological hurdles. Its policies towards encrypted data fall into this category.

C. ENCRYPTION POLICY IN CHINA

Due to the strong influence of the government, as explained in the previous section, Chinese processes are driven almost entirely by state organizations.230 The Chinese government exerts control over processes like encryption through the use of laws developed by these state organizations. These controls are in addition to criminal laws that are germane to the encryption discussion. To cover device encryption policy in China properly, these relevant areas are examined in the following sections.


230 Segal, “China, Encryption Policy, and International Influence.”
1. Regulation of Encryption

China is not a member of the Wassenaar Arrangement, but does have stringent regulations when encryption is the core function of manufactured software or hardware. China began regulation of encryption in 1999 under State Council Order Number 273, “Regulation of Commercial Encryption Codes.”\(^{231}\) The order set forth general rules and licensing, regulations of research, production, sales, and use, and the associated penalties for non-compliance.\(^{232}\) Specifically, it defined encryption products regulated within the order as those, “products and technologies used in the encoding protection or security certification of information that is not part of state Encryption.”\(^{233}\) It also designated the appropriate government regulatory authorities as the State Encryption Management Bureau and the Office of State Commercial Cryptography Administration (OSCCA).\(^{234}\)

The composition of the 1999 order, and broad definition of pertinent encryption products, allowed for the function of a broad interpretation and application of the law. The OSCCA subsequently issued clarification on issues relating to the implementation of commercial encryption. The OSCCA stated the rationale behind their updated guidance as a result of, “The relevant departments of the Chinese Government [that] are mindful of the concerns felt in commercial circles in some countries with regard to the [Regulation of Encryption Codes].”\(^{235}\) The OSCCA indicated that software and hardware whose core function was encryption were to be regulated while information and communication technology (ICT) products that applied encryption, like cellular phones or laptops, would

---


\(^{232}\) Asian Legal Information Institute, “Regulation of Commercial Encryption Codes.”

\(^{233}\) Asian Legal Information Institute.

\(^{234}\) Asian Legal Information Institute.

\(^{235}\) ChinaECLaw, Issues Relating to the Administration of Commercial Encryption.
not fall within the scope of this order. Some researchers pointed out, “these statements did not amend the Encryption Regulations but rather indicated how the government intends to enforce them.” Further, they claim that the guidance was issued by a subordinate government agency, and that the government’s intentions could change. However, no evidence is available to indicate that the government ever deviated from the OSCCA’s stated intentions.

Since 2000, attempts have been made to include ICT products in encryption regulations indirectly, primarily through infrastructure compliance, but most of these attempts have all been met by strong international consternation and were eventually abandoned by the Chinese government. The most significant and noteworthy attempt impacted wireless products. In 2003, China banned 802.11 WiFi due to national security concerns. This ban was significant, because the government attempted to force companies to accommodate only a wireless local area network (WLAN) authentication and privacy infrastructure (WAPI) encryption technique. The United States Trade Representative’s (U.S.T.R.) 2004 Report to Congress on China’s WTO Compliance and a letter from U.S.T.R. Zoellick, U.S. Secretary of State Powell, and other U.S. administration officials articulated concern about China’s course of action. In April 2004, following trade discussions with the U.S.T.R., Chinese Vice Premier Wu Yi announced the government would indefinitely postpone the WAPI standard as a result of

---


237 Cloutier and Cohen, “Casting a Wide Net.”

238 Cloutier and Cohen.

U.S. pressure. This postponement did not occur before Apple complied, and introduced an iPhone model supporting both WiFi and WAPI. This episode is relevant for two reasons. First, it illustrates China’s continued attempts to control the type of encryption its citizens are able to access in the non-commercial arena. Second, it shows the willingness of a multinational corporation like Apple to acquiesce to the demands of the Chinese government.

So far, encryption-specific regulation in China has remained a matter of industrial policy. China has floated draft legislation for comment on multiple occasions requiring source code for ICT products to be submitted for review. Possessing the source code would not allow for decryption, but would assist the government in moving more quickly to that end. Facing this opposition, China has opted to address the issue directly by passing a law to compel companies to assist with decryption (discussed in the following section).

2. Laws Directly Impacting Device Encryption and Exceptional Access

As encryption concerns returned to the forefront of the international agenda over the past three years, China’s National People’s Congress made the decision to legislate directly on the issue. The government’s actions on encryption have set China apart from countries across the world.

In December 2015, the government enacted the Counter-Terrorism Law of the Peoples Republic of China. A draft version released in 2014 contained language that


would have required telecommunications companies to install backdoors and provide encryption keys. No country’s government had taken such an extreme stance on exceptional access other than the United States during the Crypto Wars in the 1990s. The draft legislation stated, “Telecommunications operators and internet service providers shall install in the design…and report cryptography schemes to departments responsible for encryption for examination.”\textsuperscript{243} Failure to comply with the law would have resulted in the termination of service for companies in China. The final version adopted at the end of 2015 lacked the initial language, and instead, included softer language, which made the only requirement for companies, “assistance.”\textsuperscript{244} Article 18 of the enacted law stated:

\begin{quote}
Article 18: Telecommunications operators and internet service providers shall provide technical interfaces, decryption and other technical support assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities in accordance with law.\textsuperscript{245}
\end{quote}

In response to its passage, Li Shouwei, deputy head of the NPC’s criminal law division under the legislative affairs committee stated to local press, “[It] will not affect companies’ normal business nor install backdoors to infringe intellectual property rights, or ... citizens freedom of speech on the internet and their religious freedom.”\textsuperscript{246} A literal reading of the law indicates that Shouwei’s statements are factually accurate insomuch as the law does not call for techniques like key escrow or other means of exceptional access. However, the legislation still calls for technical assistance and decryption from companies, something no other country has mandated. Further, the stated limitations of the law to the investigation of terrorist activity, reiterated by Shouwei in his statement, could be disingenuous. As one researcher states, based on the comments of Chinese dissident activist Hu Jia, “there is enough scope for creating ‘emergency situations’ in


\textsuperscript{244}China Law Translate, “Counter-Terrorism Law (2015).”

\textsuperscript{245}China Law Translate.

order to restrict the rights of the people or heavily suppress any local dissent.” These two issues are discussed more comprehensively in the following paragraphs.

The questions remain, will companies comply with this law and in what circumstances will they be called upon? Neither question can be empirically answered at this point. If Chinese law enforcement has chosen to call upon the assistance of telecommunications companies, neither party has publicly disclosed that information based on the research conducted. Both questions can be addressed on a theoretical level but even this situation leaves a nebulous understanding of its potential.

Addressing the latter question, the law was written to counter terrorism, and accordingly, the circumstances upon which this law would be used presumably revolve around such an act. To that end, the law defines terrorism in Article 3 and states:

“Terrorism” as used in this Law refers to propositions and actions that create social panic, endanger public safety, violate person and property, or coerce national organs or international organizations, through methods such violence, destruction, intimidation, so as to achieve their political, ideological, or other objectives. The definition, especially with the use of the phrase, “other objectives,” and in the context of a country that elevates the sanctity of its ruling party to the highest level in law, leaves the door open for almost unlimited use. The previously cited analysis draws similar conclusions.

With regard to compliance, research revealed that no companies publicly stated that they would not comply. Further, it is only necessary to look to the historical decisions of companies in related areas to know that if called upon, they will likely provide whatever assistance is requested. The opportunities for technology adoption and consumer growth in China are far too great for any competitive multinational company to risk losing business in that country. According to researchers:

---


248 China Law Translate, “Counter-Terrorism Law (2015).”

The Internet was an American invention and it was in the Western context that the technology was built and matured, but US users no longer drive online developments. China’s online population surpassed that of the United States in 2008, and today there are more Chinese Internet users than there are Americans on the planet. With more than half the Chinese population still offline, this shift in the Internet’s centre of gravity is likely to continue to accelerate over the next decade.250

Companies like Apple already showed a willingness to comply in 2006 when China required wireless devices to be WAPI compliant. In fact, Apple CEO Tim Cook was recently quoted as saying, “like we do in other countries, we follow the law wherever we do business.”251 This comment was relative to a decision by Apple to remove virtual private network (VPN) applications from its online stores in July 2017 at the request of the Chinese government. An October letter from Senators Ted Cruz and Patrick Leahy questioned this decision.252 This latest move by Apple to meet the legal requirements of China came on the heels of its decision to open up local data centers in China to comply with an additional Chinese cyber law that went into effect on June 1, 2017 that required online data of its citizens to be stored within Chinese territory.253

Multiple sources have reported that Apple is not alone in its willingness to meet China’s demands. Microsoft released a similar statement in 2014, stating, “Microsoft complies with the laws and regulations of every market in which we operate around the world…Our business practices in China are designed to be compliant with Chinese law.”254 In 2005, Microsoft shut down the blog of a Chinese free speech advocate.255 In


255 Parker, “Apple Caved to China, Just Like Almost Every Other Tech Giant.”
2006, Microsoft, Google, Cisco, and Yahoo representatives appeared in a congressional hearing to answer questions about their questionable collaboration with the Chinese government. In 2014, LinkedIn debuted in China with the caveat that users’ information displayed in that country may be filtered based on content. These are only some of the examples of ongoing compliance due to what some have cited as the Chinese government using, “its country’s vast market at leverage over American technology companies.” While reports of companies capitulating to the Chinese government’s counter-terrorism law have not surfaced recently, it is reasonable to surmise that these same companies would take similar actions if called upon to assist.

3. Stored Information Laws in China

The Criminal Procedure Law of China was initially adopted in 1979, with amendments in 1996 and 2012. Some argue it was done in haste, and the country should have been more deliberative in its establishment of criminal laws and procedure. The basis of criminal law in China can be found in the Constitution and its criminal procedure law. Within those areas, this section looks at the content and implementation of search and seizure laws, as well as those affecting electronic evidence to understand the encryption policy of China better.

The basis of law in China is rooted in its Constitution. As previously discussed, the focus of the Constitution is on preserving government and the socialist party. It is important to note that Article 5 of China’s Constitution states that the Constitution and China’s laws take precedence over all individuals. The only reference to search and seizure falls within articles 37 and 39, which references searches of people and homes, respectively. An actual search of a person, as stipulated in Article 37, is almost an after-

---

256 Parker.
257 Parker.
thought as it states at the ends of the law, “and unlawful search of the person of citizens is prohibited.”\textsuperscript{260} This article is most comparable to the Fourth Amendment of the U.S. Constitution but lacks the substance and parameters found in U.S. jurisprudence.

The criminal procedure law provides the basis for criminal law in China. The Criminal Procedure Law of 2012 includes general provisions about evidence, protocols for filing a case and investigation, as well as trial procedures and special procedures. Within Part II, Chapter II, Sections 5 and 6 are the guidelines for searches and seizures during criminal investigations. Unlike legal rules set forth in the United States, the sections briefly lay out these protocols. In Section 5, which pertains to searches, Article 134 states, “In order to collect criminal evidence and track down an offender, investigators may search the person, belongings and residence of the criminal suspect and anyone who might be hiding a criminal or criminal evidence.”\textsuperscript{261} Article 136 states, “When a search is to be conducted, a search warrant must be shown to the person to be searched. If an emergency occurs when an arrest or detention is being made, a search may be conducted without a search warrant.”\textsuperscript{262} Within the sections pertaining to evidence, language supports procedures relative to electronic evidence added in 2012. Article 48 of Chapter 5 states, “All materials that prove the facts of a case shall be evidence. Evidence shall include…audio-visual materials, and electronic data.”\textsuperscript{263} Article 52 further stipulates, “The physical evidence, documentary evidence, audio-visual materials, electronic data and other evidence gathered by administrative organs during administrative law enforcement and case investigation and handling may be used as evidence in criminal cases.”\textsuperscript{264} Amongst the evidence guidelines are also exclusionary rules, which have not always been present in Chinese law.

\textsuperscript{260} Zheng.


\textsuperscript{262} National People’s Congress of the People’s Republic of China.

\textsuperscript{263} National People’s Congress of the People’s Republic of China.

\textsuperscript{264} National People’s Congress of the People’s Republic of China.
The laws protecting information stored on devices in China are, in appearance, similar to those in the United States under the Fourth Amendment of the U.S. Constitution. Citizens of China have legal protections set forth in the constitution and criminal procedure law. In this way, the legal structure of criminal law in China is similar to the United States on a superficial level.

4. Political and Religious Repression and Human Rights Abuses

A conversation about the legal protections of Chinese citizens should also include the lack of protections people have in practice. The government of China has a record of political and religious repression and human rights transgressions. Many of these have been documented as being carried out by the Ministry of Public Safety.

According to Amnesty International, over the past year, China continued to systematically monitor, harass, intimidate, detain, and arrest political and religious activists. Numerous examples have been documented and include the arrest and conviction of activist Zhai Yanmin for subverting state power, the detention of pro-democracy activists Jiang Yefei and Dong Guangping, and the arrests and convictions of pastors Bao Guohua and his wife, Xing Wenxiang, who had been vocal in preventing the removal of crosses from churches, for gathering a crowd to disturb social order.

Actions authorized by the counter-terrorism law raise additional concerns. “Religious repression conducted under ‘anti-separatism’ or ‘counter-terrorism’ campaigns remained particularly severe in Xinjiang Uighur Autonomous Region and in Tibetan-populated areas.” Human Rights Watch (HRW) documents similar instances

---


268 Amnesty International.

269 Amnesty International.
in its 2016 World Report and also highlights more severe human rights infractions.\textsuperscript{270} In fact, HRW responded to initial drafts of the counter-terrorism bill by stating that

the law would legitimate ongoing human rights violations and facilitate future abuses, especially in an environment lacking basic legal protections for criminal suspects and a history of gross human rights abuses committed in the name of counterterrorism. Such violations are evident across the country and particularly in the Xinjiang Uyghur Autonomous Region, the region that has been most affected by acts of terrorism and political violence in recent years.\textsuperscript{271}

Further, HRW and other groups present empirical evidence linking political repression and human rights abuses to law enforcement. In 2008, the United Nations Committee against Torture concluded, “notwithstanding the State party’s efforts to address the practice of torture and related problems in the criminal justice system, the Committee remains deeply concerned about the continued allegations...of routine and widespread use of torture and ill-treatment of suspects in police custody.”\textsuperscript{272} HRW conducted comprehensive research of over 400 verdicts in the first quarter of 2014. Their analysis showed that, “police torture and ill-treatment of suspects in pre-trial detention remains a serious concern.”\textsuperscript{273} They also found, “Former detainees described physical and psychological torture during police interrogations, including being hung by the wrists, being beaten with police batons or other objects, and prolonged sleep deprivation.”\textsuperscript{274} The U.S. State Department states:

Despite legal protections [afforded by the constitution], authorities often do not respect the privacy of citizens in practice. Although the law requires warrants before law enforcement officials can search premises, this provision frequently has been ignored; moreover, the Public Security


\textsuperscript{274} Human Rights Watch China Team.
Bureau and the procuratorate can issue search warrants on their own authority.\textsuperscript{275}

The reported abuses referenced previously are of particular concern as they apply to the MPS, which is the authority responsible for issues of device encryption. Based on the guidelines of the law, MPS personnel will likely be calling telecommunications operators and internet service providers for decryption assistance in the name of terrorism, as they choose to define the term. At this point, no evidence has indicated that the law has been used to compel decryption assistance to support political or religious repression or human rights abuses. However, it is worth noting that Article 90 of the Counter-Terrorism Law of 2015 includes verbiage restricting many reporting details of terrorist incidents and counter-terrorism responses; failure to follow this guidance results in specified fines and detention.\textsuperscript{276} This section of the law, along with other policies of state controlled information flow within China, makes it unlikely that open reporting on the utilization of the decryption assistance clause will occur.

Based on the analysis of the United Nations, HRW, and Amnesty International, although the laws of China appear to offer protection for civil liberties like those of the United States, the reality is much more grim. Unlike Israel and the United States, China received low rankings from the independent watchdog organization, Freedom House, in categories used to assess civil liberties in the country.\textsuperscript{277} The ratings contribute to the overall opinion that the country is not free. The Chinese government, using its various state organs, will go to extreme lengths to maintain a perception of control, even if it means abusing the religious, political, or human rights of its citizens.

D. CONCLUDING THOUGHTS

When presented with the issue of device encryption, China has a centralized, structural approach through its forensic unit in the MPS. The government also relies on

\textsuperscript{275} United States Department of State, “Country Reports on Human Rights Practices, February 23, 2001, China.” The Supreme People’s Procuratorate is the PRC’s highest agency at the national level responsible for both prosecution and investigation.

\textsuperscript{276} China Law Translate, “Counter-Terrorism Law (2015).”

partnerships with academia and the private sector to bolster Chinese law enforcement’s abilities. However, based on China’s decision to pass the Counter-Terrorism Law of 2015, those structural efforts appear to be secondary to compulsion. China took the unprecedented step to require companies legally to assist with decryption, or technical support to that end, which is the crux of their approach to encryption.

China has demonstrated a historical pattern of gaining compliance from companies operating in China through legal means, and the counter-terrorism law is another step in that direction. Although China has capitulated to international pressure in past cases, postponing or suspending passage of potential laws that met with great concern or resistance, once these laws are passed, companies have also shown a pattern of compliance. The government has learned that companies with a desire to operate in the market share China has to offer are willing to abide by laws passed, no matter how unreasonable they may be to the values of the companies or critics across the world.

It is reasonable to conclude that as the government of China matures, it is attempting to establish legitimacy through legal frameworks like the criminal procedural law, even as it continues to require the ability to access encrypted devices that may belong to individuals seen as threats to the government or the socialist party. To maintain this appearance, laws like the Counter-Terrorism Law of 2015 are necessary, as they are complementary to the already existing frameworks.

Within this context of law enforcement and encryption, China’s record of political, religious, and human rights abuses must be accounted for in this analysis. In cases touching political issues or powerful groups, China’s ruling communist party maintains instruments to subvert legal and judicial processes. According to one watchdog organization, “While citizens can expect a degree of fair adjudication in nonpolitical cases, those that touch on politically sensitive issues or the interests of powerful groups are subject to decisive ‘guidance’ from political-legal committees.” The Counter-Terrorism Law of 2015 strengthens this image of fair adjudication in

\[278\] Freedom House.
\[279\] Freedom House.
nonpolitical cases, and may eventually be used to enhance the image of actions in politically sensitive ones. Presently, it is more indicative of the Chinese government’s continued capacity to exert power over those with whom it has contact when it so chooses. The structural features of the Chinese approach, as well as a legal mandate for exceptional access, are lacking in the United States. In practice, this legal structure provides much less protection for civil liberties than in the United States, while it legitimates compelling private companies to provide decryption support to practices that repress individual liberty. However, the use of a legal mandate to compel access does not automatically trigger the repression of rights, although in China, conceivably this law was passed for this very reason.

These factors are important to consider when assessing a solution to the U.S. debate on the issue. Based on comments and actions from telecommunications companies operating in China, they appear willing to comply with the legal requirements set forth by the government. It is possible that in the face of legal pressure, the same response would be seen in the United States. The next chapter provides an analysis of both structure and legal means to gain exceptional access for the United States based on the lessons learned from Israel and China.
V. ANALYSIS OF ENCRYPTION POLICY IN ISRAEL AND CHINA FOR U.S. IMPLEMENTATION

The Master said, When I walk along with two others, they may serve me as my teachers. I will select their good qualities and follow them, their bad qualities and avoid them.280

—Confucius

The previous two chapters comprehensively covered the approaches to device encryption in Israel and China. The two approaches have some similarities in the structure of their centralized law enforcement efforts. However, Israel appears to be content with the abilities and partnerships of its cybercrime unit, while China has taken the additional step to pass legislation compelling assistance from telecommunications providers. These approaches present two options for examination for the U.S. government, which still seeks a definitive solution for the general issue of encryption.281

Building on the prior two chapters’ cases studies of Israeli and Chinese decryption policies, this chapter evaluates potential implementation of the policies of Israel and China in the United States. For each country, the chapter utilizes qualitative analysis to assess applicability by four criteria: legality, cost, political acceptance, and the potential for success for application within the United States. The focus is on what each country’s primary approach to the encryption issue can offer for reconciling debate over U.S. policy.


A. ANALYSIS OF THE IMPLEMENTATION OF THE ISRAELI APPROACH IN THE UNITED STATES

The Israeli approach to device encryption is addressed through forensic extraction by the Israel Police cybercrime unit, which has strong partnerships, built on a national consensus of security. It represents a unified, active effort by Israeli law enforcement to access data that would be otherwise untouchable through preexisting vulnerabilities. The assessment of the Israeli approach focuses on forensic extraction through the implementation in the United States of a structural solution like the federal cybercrime unit that exists in Israel. The results of the analysis are used to determine the viability of a specific proposal to create a capacity with similar characteristics in the United States.

The cybercrime unit in Israel is an entity under a unified command of the Israel Police, in which a centralized forensic laboratory specializes in extraction with a network of cyber officers throughout Israel serving individual communities. Two key differences between Israel and the United States must be accounted for prior to an analysis for proposed adoption, size and law enforcement structure. Israel is significantly smaller than the United States in both population and geography. Israel also has one police force, whereas the United States has hundreds of federal, state, and local law enforcement entities. As a result, any U.S. option that attempts to replicate characteristics of the Israeli approach will need to scale up to account appropriately for size, and consider a task force structure to accommodate a difference in law enforcement structure, since neither of those U.S. factors will realistically change.

With these two key differences taken into account, the following discussion assesses the applicability of the Israeli model in the United States on the basis of the four criteria of legality, cost, political acceptance, and the potential for success in its application.

1. Legality

In evaluating the constitutional and legal implications for implementation of Israel’s approach within the United States, no known legal barriers exist to the formation of a cybercrime unit focusing exclusively on encrypted data extraction from devices.
Some federal and local law enforcement agencies in the United States already have laboratories with device data extraction capabilities. In fact, both the FBI and the Secret Service maintain forensic laboratories across the country with a general focus on cyber forensics. The FBI coordinates about 16 RCFLs through the national RCFL program with a coordinating program office in Washington, DC.\textsuperscript{282} The Secret Service maintains approximately 40 ECTFs around the country, each with a forensic lab in the field office from which the respective ECTFs operate.\textsuperscript{283} These ECTFs are discussed in greater detail in the conclusion of this thesis, in light of the analysis of this chapter.

The formation of a singular, centralized unit, and any formal partnerships it has with academia and the private sector, would require agreements and memoranda of understanding between government departments and agencies, state and local law enforcement departments, businesses, and academic institutions. These would be administrative measures, not necessarily authorized by law, to allow the entities to work together and maintain respective equities.

The goal of these labs would be to defeat any barriers to device data extraction like encryption. The forensic techniques that might be utilized in these labs could give pause to prosecutors and judges. An argument has been put forth that in the United States, encrypted data extraction, known in some cases as ethical hacking, will require legislative changes and greater oversight. One researcher stated, “I recommend that policymakers adopt legislative actions to legalize and thereby legitimize hacking by law enforcement in limited cases as a middle-ground solution.”\textsuperscript{284} New legislation however may not be needed. In fact, many U.S. law enforcement agencies already partner with a


\textsuperscript{284}Nguyen, “Lawful Hacking,” 68.
company like Cellebrite to extract encrypted information from devices, which runs counter to this postulate calling for legislative change.  

The strongest legal argument in opposition to this approach that could be found is less legislatively based and more procedurally based. The District Attorney’s Office in Manhattan argued in a white paper on the subject of device encryption that data obtained through hacking may be difficult to introduce as evidence:

Introducing into evidence data that has been obtained through hacking or other means not provided by the operating system manufacturer may be more difficult than introducing into evidence data that is obtained through a process that was designed by the smartphone manufacturer or operating system supplier, because there may be significant questions about the authenticity, integrity and completeness of the information that has been obtained through hacking.

While this argument has some level of merit, it does not preclude the Israeli approach or ethical hacking on a legal basis. The introduction of forensic techniques and evidence almost always requires testimony on the part of a forensic examiner. Accreditation of these labs and their methods would also help to ease this burden.

A stronger argument supporting the approach can be found by extrapolating from existing law. A mobile device is a storage medium within which potential evidence of a crime may be located. The DOJ is extremely clear about this fact in its opinions in reference to obtaining electronic evidence. It is comparable to a private residence, in which items of evidentiary value are stored. In the United States, for the government to

---


gain access and search a property belonging to an individual where a reasonable expectation of privacy is protected by the Fourth Amendment, a few conditions must be met. These conditions, outlined under Rule 41 of the Federal Rules of Criminal Procedure, include obtaining a lawful warrant from a duly sworn magistrate; to do so, an investigator must show probable cause that it contains evidence of a crime. Once that lawful warrant is obtained, few limits are placed on agents of the government as to how they enter that house. They can knock on the door or they can cut a hole in the side of the house if they find that the common points of entry are impenetrable. The same is true of an electronic storage device. Once a warrant is obtained, the method law enforcement uses to gain access is reasonably without bounds. Little difference exists between whether an officer takes notes and photos sifting through applications on a device, as any other user would, or a forensic examiner makes an image of the data or gains access through a technique like chip-off forensics, Joint Test Action Group (JTAG) forensics, cold booting, or forcing an unencrypted backup to access data on a locked cell phone. As long as the government adheres to the guidelines of the search warrant, a high degree of equivalency exists. No legislative fixes or additional oversight are necessary to alter a proven, well-adjudicated process.

In fact, additional protections are offered by the Sixth Amendment as it applies to this approach. The Sixth Amendment states, “the accused...shall enjoy the right...to be informed of the nature and cause of the accusation; to be confronted with witnesses against him.” As a result of this amendment, for any evidence obtained from an encrypted device, the government must be prepared to testify to it. Presumably, this responsibility of expert testimony in this instance would fall to the forensic examiner who

289 e.g., time of day, no knock.
290 In fact, fewer limits are applicable, as no limits are placed on the time of day or announcing entry.
accessed the device. Rule 702 of the Federal Rules of Evidence prescribes requirements for those giving such testimony. The forensic examiner may be called upon to attest to the evidence being presented, and may even have to explain the technique used. In a way, it is an oversight process of ethical hacking.

Based on this analysis, no legal barriers appear to exist to standing up a centralized forensic unit to extract information from an electronic device. Federal interagency task forces already exist in cities throughout the country without any authorizing legislation. Extracting encrypted information on select devices happens on a regular basis with equipment or assistance from the Israeli-based company, Cellebrite. In fact, an argument can be made that the encryption issue is already being addressed through contracts with companies like Cellebrite. However, this dependent approach lacks efficiency, good stewardship of taxpayer dollars, and the ability to be adopted universally and equitably throughout the country.

2. Cost

Cost of the implementation of Israel’s approach to encryption is assessed on two levels, the anticipated impact on U.S. taxpayers vis-à-vis government expenditures and repercussions for U.S. businesses.

a. Impact on U.S. Taxpayers

U.S. taxpayers are spending millions of dollars for federal, state, and local agencies on solutions to device data extraction. Federal agencies like the FBI partner with Cellebrite, the company that has cornered the market on extracting encrypted data, and have spent millions of dollars on contracts with them. According to one source, since 2007, over $40M has been obligated to Cellebrite from the federal government. Meanwhile, Table 2 shows money paid by 20 states to Cellebrite for products from 2010 through 2016.

---

294 General Services Administration, “Federal Procurement Data System”; Evans, “Cell Phone Forensics.”
Table 2.  Monies Paid by 20 State Police Agencies to Cellebrite from 2010–2016.\textsuperscript{296}

<table>
<thead>
<tr>
<th>State</th>
<th>Amount in USD Paid to Cellebrite for Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arizona</td>
<td>$227,885</td>
</tr>
<tr>
<td>California</td>
<td>$16,659</td>
</tr>
<tr>
<td>Colorado</td>
<td>$26,216</td>
</tr>
<tr>
<td>Delaware</td>
<td>$45,327</td>
</tr>
<tr>
<td>Illinois</td>
<td>$111,674</td>
</tr>
<tr>
<td>Iowa</td>
<td>$258,230</td>
</tr>
<tr>
<td>Kentucky</td>
<td>$72,887</td>
</tr>
<tr>
<td>Maryland</td>
<td>$11,194</td>
</tr>
<tr>
<td>Missouri</td>
<td>$149,425</td>
</tr>
<tr>
<td>Nevada</td>
<td>$695</td>
</tr>
<tr>
<td>New Hampshire</td>
<td>$47,886</td>
</tr>
<tr>
<td>New Jersey</td>
<td>$218,867</td>
</tr>
<tr>
<td>New Mexico</td>
<td>$33,390</td>
</tr>
<tr>
<td>North Carolina</td>
<td>$158,099</td>
</tr>
<tr>
<td>North Dakota</td>
<td>$47,948</td>
</tr>
<tr>
<td>Ohio</td>
<td>$75,659</td>
</tr>
<tr>
<td>Rhode Island</td>
<td>$47,886</td>
</tr>
<tr>
<td>Tennessee</td>
<td>$2,198</td>
</tr>
<tr>
<td>Vermont</td>
<td>$96,978</td>
</tr>
<tr>
<td>Washington</td>
<td>$59,159</td>
</tr>
</tbody>
</table>

As Table 2 illustrates, hundreds of thousands of dollars are being spent by these states on device extraction assistance. However, the alleged cost to unlock an individual phone or obtain an annual subscription is not within most local and state police departments’ budgets. According to one source, the cost to unlock an iPhone is $1,500 and an annual subscription can be as much as $250,000.\textsuperscript{297} This price is consistent with the research of federal government contract actions for comparable amounts. Reviewing the previously referenced data from contracts between Cellebrite and the Department of


Homeland Security (DHS), a two-year, “Forensic Extraction Device Award,” was fulfilled at a cost of $448,087.298

Centralizing these decryption efforts under one U.S. unit specializing in device data extraction could be a significant benefit to the taxpayer. Costs associated with this venture will be incurred, and they may initially exceed current amounts being spent on companies like Cellebrite during the implementation of a new forensic program. However, in the same way that many local and municipal law enforcement organizations obtain forensic assistance from state-run laboratories to save on the costs of having their own independent forensic resources, decryption and extraction efforts from one centralized unit could eventually yield similar benefits.

While Congress need not statutorily authorize the centralized U.S. cybercrime unit described, it will still require appropriations. As mentioned previously, initial costs could be significant before normalizing. The services, should they be provided under federal leadership to state and local partners, will attract federal money; an area in which partnerships will be critical. The unit, like Israel’s, should be able to derive its knowledge on decryption and data extraction from law enforcement specialists, U.S. businesses, and academia, instead of a multinational cybersecurity business like Cellebrite. Even if forensic experts deem the products of a company like Cellebrite too valuable to break this relationship, centralizing tools from such a company in designated federal facilities could be advantageous. Making these tools available to state and local departments through smaller regional laboratories, instead of paying for hardware and software subscriptions themselves, would likely be a cheaper and more effective option to the current decentralized efforts.

Funding sources, mechanisms, and motivation to direct monies to cyber challenges are already present in the United States. A forensic task force will likely cause much of the money being directed to companies like Cellebrite to remain in the country, as the knowledge base of such a unit increases in the area of decryption and extraction.

This approach could also ease any fiscal burden on state and local police departments that choose to seek their own solutions unilaterally.

b. **Impact on U.S. Businesses**

The cost to U.S. businesses is another factor that must be considered with this approach. The Israeli approach provides a solution that may benefit U.S. businesses. A dedicated law enforcement unit focused on breaking the encryption of devices will force companies to stay on the cutting edge of encryption technology. According to the vulnerabilities equities process, once the government uncovers a vulnerability, the circumstances and vulnerability are presented to a board of government agency representatives where a determination is typically made to disclose its existence to the affected company.\(^2\) Assuming a determination is made to alert the company, it will allow the company to patch or prevent an exploit from being used again. This approach creates a cycle of improvement and innovation.\(^3\) The company will benefit financially by being able to tout its ability to keep its user information safe following the discovery of vulnerabilities. Meanwhile, technologists argue that this method will also ultimately benefit a forensic unit, as it will have to adapt and increase its knowledge base once the exploit is secured.\(^4\) In addition, it is also possible that such a relationship will increase cooperation between the private and public sectors. Either way, such an approach seems unlikely to hurt U.S. businesses.

On a more speculative level, should a forensic unit in the United States successfully leverage the talent of those in academia as it does in Israel, U.S. companies stand to benefit if those workers migrated to the private sector. The advantages that U.S. companies would reap from enhanced technological developments and innovative projects of skilled workers who join the workforce following hands-on experiences in academic institutions that partnered with the government could be significant. For


\(^3\) Bellovin et al., “Lawful Hacking,” 31; Manhattan District Attorney’s Office, Smartphone Encryption and Public Safety, 7.

\(^4\) Bellovin et al., 31.
example, the NSA already takes advantage of such partnerships with its National Centers of Academic Excellence in Cyber Operations Program, touting these collaborations as accelerating mission solutions, and many NSA alumni have gone on to make a significant impact in the private sector.302

The costs associated with the Israeli approach are likely to break even with current expenditures with the probability of benefiting U.S. businesses and economy. It is likely that initial start-up costs for law enforcement to access devices should hold steady with the possibility of increasing as a forensic unit is stood up. However, like most ventures, these costs should level following their establishment, and the centralization of efforts should benefit an untold number of federal, state, and local organizations. The approach has the potential to benefit U.S. companies in a few areas, and with the money for decryption remaining in the country, the overall benefit to the economy should also be positive.

The degree and nature of achieved cost efficiencies within government and benefits to private businesses depends on the details of how a forensic task force is organized and implemented. While the preceding assessment identifies several opportunities for savings and benefits, careful analysis of these factors is a necessary step in the further development of this option.

3. Political Acceptance

Political acceptance of the Israeli approach is evaluated on the expected reception of two groups, the legislative branch and the U.S. population. Acceptance by the legislative branch can be measured by the likelihood of approval or willingness to initiate legislative action based on previously exhibited behavior. The expected reception of the

U.S. population can be assessed through previously administered public opinion polls on related issues.

a. **The Legislative Branch**

The U.S. Congress is constantly tackling significant issues like cybersecurity or encryption. Chairman Michael McCaul attempted to create a more unified and operational approach to cybersecurity in the DHS over the past two years with his legislation, the *Cybersecurity and Infrastructure Security Agency Act*. Notably, a search of current and past legislation indicates no efforts have been made to authorize statutorily a centralized forensic task force unit modeled after the Israeli system. However, a lack of authorization does not prohibit someone from operating under existing laws, which may be the most politically appealing aspect of a U.S. cybercrime unit. The Secret Service’s National Computer Forensic Institute, for example, only received authorizing language in October 2017, but it has been in existence for almost a decade, and provides cyber training to state and local law enforcement officers and others.

The formation of a U.S. cybercrime unit would ease the calls for Congress to address encryption from privacy and exceptional access advocates alike, because it is a solution that helps satisfy both groups’ demands. As previously discussed, the issue of exceptional government access has been a topic of discussion on the Hill and in the Executive Branch for decades. Some Senators and Congressmen called for greater exploration on the matter, while others adamantly opposed government intervention on the issue; the Clinton Administration even attempted to provide a solution with the controversial Clipper Chip. A forensic task force unit would provide a solution amenable to all parties in the encryption debate and eliminate the need for further congressional action. Technologists in favor of privacy, but respectful of the belief that

---


law enforcement may need to access certain encrypted information, have already made the argument for law enforcement to exploit security flaws. Those supporting the position of exceptional access would likely find satisfaction with the creation of a unit focusing solely on encryption and device data extraction, provided access to devices are able to be achieved. To be clear, those in support of exceptional access like Manhattan District Attorney Vance have made it clear that they would prefer a solution that involves industry assistance. However, given the present stalemate, the option of hacking encryption is also already being exercised unilaterally by the Manhattan DA’s office, which is a clear indication it will not be opposed to such actions.

The idea of a unified cybercrime unit satisfies many of the encryption arguments from both sides of the debate over the past few decades. Since these groups are typically the catalyst for Congressional involvement and intervention on the subject, it is reasonable to believe that the Israeli model would find acceptance in the legislature. That such a task force will not require Congressional statutory authorization or compel access using other means makes it even more politically palatable.

b. The U.S. Population

Relative to the expected reception of the U.S. population, it is worth revisiting the conclusions drawn in Chapter III about Israel. Israel’s sociocultural security environment is a key factor in the basis of its device encryption policy. The Israeli population’s shared experience in the military and recognition of enemies at its borders establishes a common mindset of national security through the Israeli security network. Homogeneity exists in thought on subjects of security and counter-terrorism, and these are intrinsic. The country’s law enforcement entities are able to take advantage of this mindset in its application to criminal investigations and acceptance of their methods.

---

305 Bellovin et al., “Lawful Hacking,” 5.
306 Manhattan District Attorney’s Office, Smartphone Encryption and Public Safety, 31–33.
The United States, a country of inhabitants hailing from different cultures, countries, and backgrounds, does not have this common thread running through its population. As a result, the challenge in the United States is participation and acceptance by a population leery of the potential for government overreach and law enforcement’s abuse of power. For example, a poll taken in the last five years found the majority of the country believes, “that federal courts fail to provide adequate limits on the telephone and Internet data the government is collecting as part of its anti-terrorism efforts.”

This is not to say that public support for the Israeli approach is unattainable because the same level of homogeneity does not exist in areas of security and counter-terrorism in the United States. This support can be accomplished by highlighting the types of criminal cases that will be prioritized like terrorism, homicides, assaults, human trafficking, and sexual exploitation. Many of these issues typically transcend cultural differences, with terrorism ranking at the top of the U.S. public’s policy priorities in 2018. Law enforcement organizations affiliated with a forensic unit in the United States may also need to distance their efforts publicly from the intelligence community. Unlike intelligence agencies, the techniques used by law enforcement forensic analysts can be scrutinized in court. This level of transparency is a quality that may be more amenable to U.S. society, and prompt acceptance and participation behind a common cause.

More importantly, as the world settles into a digital existence, a generation in the United States is coming of age that has never lived a day without the internet. Passcode, a project started by The Christian Science Monitor in 2014 to provide insight into the challenges of the Digital Age, sought out 15 rising stars in cybersecurity under the age of 15. In conducting interviews of these young adults, interviewers found almost all of them supported white hat hacking for the betterment of their digital society. “The kids all


had a strong sense of ethics—and a desire to create a safer digital future for their peers.”

The potential for the support of the Israeli approach to defeat device encryption ethically in the name of altruism may only grow, as the views of the next generation of young adults come to dominate public opinion in the United States.

Through clear messaging and a reasonable framework of the mission of a forensic task force unit, and a growing proportion of the populous who understands the complications, ethics, and bounds of a digital society, prospects are strong that U.S. society will accept and even actively participate in the Israeli model implemented in the United States.

4. Potential for Success

Based on the literature and research on the subject, success is multi-faceted. First, does the method employed resolve the privacy versus exceptional access debate? To move on from the debate, this condition must be satisfied. Second, does the method employed result in the ability of law enforcement to obtain usable data from a device that was once encrypted? This aspect is critical when relying on the structural methods used by the Israel Police cybercrime unit.

a. The Privacy versus Exceptional Access Debate

The first criterion of success, whether the method employed resolves the privacy versus exceptional access debate, is met with the Israeli approach. On the privacy side of the debate exists two entities, technologists and civil libertarians. Both technologists and civil libertarians want to ensure strong encryption is available and prolific. Technologists believe requisite government access should do nothing to weaken encryption, and are therefore generally in favor of a lawful hacking approach. Civil libertarians support government access to encrypted information if bounded by

---


appropriate checks and balances. The Israeli approach allows for strong encryption, does not weaken encryption, does nothing to alter the status quo of the established law, and as previously discussed, may even make encryption stronger. On the exceptional access side of the debate, the government wants to ensure it is able to access encrypted information when it has legitimate law enforcement inquiries.\textsuperscript{314} The Israeli approach is the vehicle for this access, and operating under the assumption that it will be successful, it meets this requirement.

\textit{b. The Ability of Law Enforcement to Access Encrypted Information}

To satisfy the second criterion of success, the ability of law enforcement to obtain usable data from encrypted devices, many factors must fall into place. There is no reason to believe a centralized approach of law enforcement organizations with partnerships in the private sector and academia could not be as successful as in Israel. However, the U.S. context presents unique challenges and opportunities to achieving the coordination necessary for this structural approach.

Structurally, the fact that the United States does not have a centralized law enforcement agency, but many federal, state, and local agencies, will pose the greatest structural challenge for organization. Operating under the assumption that this unit would not be cause for the creation of a new federal agency, an existing federal law enforcement organization would need to lead and gain the support and participation of other federal, state, and local law enforcement organizations to be successful. This issue would require executive branch leadership. It is also not an insurmountable task, as it was accomplished previously with regards to counter-terrorism, with the creation of FBI Joint Terrorism Task Forces (JTTFs) under the National JTTF.\textsuperscript{315}


Strategically, a forensic task force stood up in the United States will also need to develop stronger partnerships with the private sector and academia. Law enforcement alone will not be able to reproduce the results in Israel without these important partnerships. Some federal agencies like the FBI and Secret Service fortunately claim to already have strong relationships with the private sector and academia.\footnote{“Office of Private Sector,” Federal Bureau of Investigation, accessed January 29, 2018, https://www.fbi.gov/about/partnerships/office-of-private-sector; “The FBI and Academia,” Federal Bureau of Investigation, accessed January 29, 2018, https://www.fbi.gov/audio-repository/news-podcasts-thisweek-the-fbi-and-academia.mp3/view; United States Secret Service, “Investigations.”} Developing these relationships further will allow them to gain access to appropriate personnel and technology to make them successful. A competent forensic unit will need individuals who have the deep technical expertise for telecommunications and computer science necessary to exploit encrypted devices.\footnote{Susan Landau, “The Real Security Issues of the iPhone Case,” \textit{Science} 352, no. 6292 (June 16, 2016): 1399, doi: 10.1126/science.aaf7708.} The unit will also need to develop or have access to innovative tools, much like the NSA, which will be accessed through these partnerships.\footnote{Landau, 1399.}

Assuming that the structure and partnerships of the Israel approach can be replicated with appropriate modification for the different U.S. context, the United States would probably be on even footing with Israel in implementing the approach successfully.

\textbf{B. ANALYSIS OF THE IMPLEMENTATION OF THE CHINESE APPROACH IN THE UNITED STATES}

The Chinese approach to encryption policy is multi-faceted. Like Israel, a centralized effort, under the Ministry of Public Security, for cyber forensics with additional device extraction occurs at local levels. Research indicates some partnerships exist with this department, but it is unclear whether they play a significant role in decryption efforts. Further, with an authoritarian government like China’s, it is difficult to know if partnerships with the government are voluntary or compulsory.
China has also legislated on the issue. Based on laws passed over the past year, the government compels decryption assistance from telecommunications operators and internet service providers under a broad definition of terrorism. No evidence indicates they have made use of the law, but multiple foreign companies have stated they will follow the laws of each country in which they operate.

Having already assessed Israel’s centralized unit dedicated to forensics, the focus of the analysis on China’s approach will rest in its decision to compel assistance through legal means.\footnote{This analysis will expand China’s approach, which on the face, is limited to terror cases. As previously argued, China’s definition of terrorism, unlike that found in the Title 18 of the United States Code, is extremely broad and may already include more generalized criminal topics. In analysis for application to the United States, this thesis operates under the assumption that any laws passed in the United States will not restrict encryption assistance only to terror given that this limitation will not adequately address the device encryption issue.} This stance is particularly important, as it appears it is an outcome still sought by some in the U.S. government.\footnote{U.S. Department of Justice, “Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy”; Department of Justice, \textit{Statement of Christopher A. Wray}.}

1. **Legality**

In evaluating the legal implications for implementation of China’s approach within the United States, on the face of it, many features would be proscribed by the U.S. Constitution. The following discussion, however, develops important additional implications beyond this basic observation.

The idea of attempting to legislate on the issue of encryption is not foreign to the United States. Following the public fight between Apple and the FBI, some members of the U.S. Congress (MOCs) chose to test the waters. In 2016, Senators Richard Burr and Dianne Feinstein circulated a bi-partisan draft bill that mirrored the language in China’s counter-terrorism law on the subject. The essence of the Burr-Feinstein discussion draft was best illustrated in one of its sections that stated:

> to uphold both the rule of law and protect the interests and security of the United States, all persons receiving an authorized judicial order for information or data must provide, in a timely manner, responsive,
intelligible information or data, or appropriate technical assistance to obtain such information or data.\footnote{Compliance with Court Orders Act of 2016, \textit{Discussion Draft}.} However, the bill was not received well by their elected colleagues, technologists, or the administration. As a result, the bill was never formally introduced. Questions do remain. Legally speaking, could such a bill be introduced and eventually be signed into law? Do the requirements placed on companies by China’s law, or something like the Burr-Feinstein draft bill, exceed Constitutional limitations in the United States?\footnote{Andrew Crocker and Jamie Williams, “Deep Dive: Why Forcing Apple to Write and Sign Code Violates the First Amendment,” Electronic Frontier Foundation, March 3, 2016, https://www.eff.org/deep-links/2016/03/deep-dive-why-forcing-apple-write-and-sign-code-violates-first-amendment.}

As explained in Chapter II of this thesis, present-day encryption relies heavily on digital signatures. Many hardware and software manufacturers have designed their operating systems only to accept code with digital signatures from those hardware and software manufacturers.\footnote{Crocker and Williams; Brief for the Electronic Frontier Foundation and 46 Technologists, Researchers, and Cryptographers, in the Matter of the Search of an Apple iPhone Seized during the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 3KGD203 (2016), 10, https://www.eff.org/files/2016/03/03/16cm10sp_eff_apple_v_fbi_amicus_court_stamped.pdf.} Technical assistance given by companies to defeat the encryption security of the device would require code that includes these digital signatures. In the Apple and FBI case, the argument was that this feature would be in violation of First Amendment rights. In an amicus brief filed by the Electronic Frontier Foundation in support of Apple, supporters of this position argued

\begin{quote}
Apple is being forced to actually write and endorse code that it—rightly—believes is dangerous. And in doing so, it is being forced to undermine the trust it has established in its digital signature…This is a clear violation of Apple’s First Amendment rights, in addition to being a terrible outcome for all the rest of us who rely on digital signatures and trustworthy updates to keep our lives secure.\footnote{\textcite{Crocker and Williams; Brief for the Electronic Frontier Foundation and 46 Technologists, Researchers, and Cryptographers, in the Matter of the Search of an Apple iPhone Seized during the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 3KGD203 (2016), 10, https://www.eff.org/files/2016/03/03/16cm10sp_eff_apple_v_fbi_amicus_court_stamped.pdf.}}
\end{quote}

Although the government vacated its case before litigation occurred, the argument has merit. Technical assistance to access encrypted data on a device would likely require code to be written and include the digital signature of the hardware or software
manufacturer; the Supreme Court already determined the First Amendment protects code, as a form of writing, in *Bernstein v. DOJ*.324

Therefore, there is room to argue that in some cases, such a law could be interpreted as violating the First Amendment of the Constitution. If the law was written in such a way to articulate that the technical assistance or decryption techniques used would not violate the First Amendment (i.e., technical assistance other than writing new code), then no foreseeable legal barriers can be seen in China’s approach or that of Senators Burr and Feinstein. Nevertheless, even with Constitutional concerns, not much can stop a MOC from drafting and introducing a bill that may discernibly exceed the Constitution.325 Only after a law is passed, and a challenge filed, would the courts be able to listen to arguments and interpret its constitutionality; this process could take years to resolve assuming that the legislative action is a change in statute and not a constitutional amendment. The reception to the Burr-Feinstein bill indicates both options appear highly unlikely to occur.

Based on this discussion, and in keeping with the scope of the Chinese approach, it appears legal barriers do exist to entry. The issue of the political acceptability aspect of this discussion is the subject of a forthcoming section.

2. Cost

The cost of the implementation of China’s approach to encryption is assessed on two levels, the anticipated impact on U.S. taxpayers vis-à-vis government expenditures and repercussions for U.S. businesses.

---


325 It is the author’s understanding that MOCs, with the support of their colleagues in the House and Senate, and the approval of the Executive Branch, have no limits in the language of the bills they file. The Office of Legislative Counsel may provide advice to MOCs on the constitutional, legal, and technical problems in proposed legislation, but it does not prevent them from filing, nor can they prevent it from becoming a law. Should the legislation become law, facial or as-applied challenges may be made by a plaintiff who believes the statute, or its application, is unconstitutional, and therefore void. See Matthew Glassman, *Office of Legislative Counsel: Senate*, CRS Report No. RS20856 (Washington, DC: Congressional Research Service, 2008), https://www.senate.gov/reference/resources/pdf/RS20856.pdf; Alex Kreit, “Making Sense of Facial and As-Applied Challenges,” *William and Mary Bill of Rights Journal* 18, no. 3, art. 4 (2010): 657–707, http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1168&context=wmborj.

95
a. Impact on U.S. Taxpayers

As explained in the previous portion of this chapter on Israel’s approach, U.S. taxpayers are already spending millions of dollars for federal, state, and local agencies on solutions to device data extraction. The adoption of a law mandating decryption support would ease the burden of many of these costs. Contracts may still be written to companies like Cellebrite for their basic device imaging technologies, but enhanced products or specialized orders would no longer be necessary.

The cost of encrypted data extraction on its face would amount to administrative costs charged by companies to the government. This cost already occurs when the government serves a court order to obtain contents of communications, records, or other information from service providers. 18 USC 2706, *Cost Reimbursement*, states:

(a)Payment.—

Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b)Amount.—

The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).\(^{326}\)

*Yahoo!*!, for example, charges the following rates for access to user information through legal processes:

---

\(^{326}\) 18 U.S. Code § 2706—Cost Reimbursement.
• Basic subscriber records: approx. $20 for the first 10, $10 per 10 thereafter

• Basic group information (including information about moderators): approximately $20 for a group with a single moderator

• Contents of subscriber accounts, including email: approximately $30–$40 per user

• Contents of groups: approximately $40–$80 per group.\(^{327}\)

Verizon, on the other hand, acknowledges that it has a right to reimbursement for law enforcement court ordered requests, but claims it does not seek it in the majority of instances.\(^{328}\)

The Feinstein-Burr draft legislation on encryption included a similar clause that stated:

\((3) \text{ COMPENSATION FOR TECHNICAL ASSISTANCE.---A covered entity that receives a court order...and furnishes technical assistance under subparagraph (B) of such paragraph pursuant to such order shall be compensated for such costs as are reasonably necessary and which have been directly incurred in providing such technical assistance or such data in an intelligible format.}^{329}\)

At this point, no known precedence exists for the cost of such assistance for encrypted data because no law currently on the books requires assistance. Based on other laws that compel assistance from service providers, allowances will likely be made for reimbursable costs. Although it is unclear what those costs may be in the instance of decryption assistance, it is reasonable to believe that it may be more affordable to the taxpayer than the price tag affixed by a company like Cellebrite for decryption. As the


\(^{329}\) Compliance with Court Orders Act of 2016, *Discussion Draft.*
Manhattan District Attorney’s Office explains, “there may be lengthy and expensive discovery battles about the hacking method that would be avoided if the data could be extracted through a means provided by the operating system manufacturer.” Instead of paying a decryption company for access to the proprietary technology or services they have developed, which can consequently be price-gouged accordingly, law enforcement would only be responsible for the administrative pricing from a device manufacturer that provides assistance. The only caveat would be if companies like Apple or Google passed the cost on to their customers, in which case, this approach might impact selected taxpayers.

**b. Impact on U.S. Businesses**

The cost to U.S. businesses is another factor that must be considered. Any law passed in the United States could impact the reputation and hinder the development of encryption and cybersecurity capabilities of U.S. companies. The prevailing argument for Israel is that its polices on encryption have launched the country into a category of top producers of this type of cyber technology while allowing it also to lead the world in the cybersecurity field of decryption. The public acceptance of laws compelling exceptional access is discussed in detail in the following sections, but data does support a negative view in the United States of companies that may allow the government to have exceptional access. In the wake of Edward Snowden’s disclosures, it was estimated that U.S. information technology businesses lost revenue ranging from $35B to $180B over three years. A program focused on legislating exceptional access to encrypted devices could have a similar impact. Such action may trigger consumers, in the United States and elsewhere, to purchase technologies produced outside of the United States that

---


331 Waxman and Hindin, “How Does Israel Regulate Encryption.”

332 “Agree or Disagree with Apple’s Decision to Oppose a Court Order to Unlock a Smart Phone that Was Used by One of the Shooters in the San Bernardino Attack?” Reuters, accessed August 15, 2015, polling.reuters.com/#poll/TM853Y16/dates/20160220-20160223/type/overall.

fall beyond the easy reach of U.S. laws. This approach would impact the revenue streams of U.S. companies.

Technologists have long made the argument that legislation requiring backdoors or assistance would lead to a weakening of encryption. Other countries or transnational criminal organizations could compromise the methods used by the companies to satisfy government regulation that ultimately would impact the reputation and revenues of U.S. companies.

The costs associated with legislation on encryption have positive and negative aspects. It is likely that costs for law enforcement to access devices would drop while their access would increase, which would be positive for those government organizations. On the flip side of this argument, legislation could introduce unforeseen costs to U.S. companies that might impact the ability of U.S. companies to remain technology leaders in the world.

3. Political Acceptance

Political acceptance of China’s approach will be evaluated on the expected reception of two groups, the legislative branch and the U.S. population. Acceptance by the legislative branch can be measured by the likelihood of approval or willingness to initiate legislative action based on previously exhibited behavior. The expected reception of the U.S. population can be assessed through previously administered public opinion polls on related issues.

a. Acceptance by the Legislative Branch

As previously discussed under the legality marker, legislating on the issue is not foreign to the United States, but neither does it appear to be palatable. As noted earlier, Senators Feinstein and Burr floated a draft of a comprehensive bill that strongly mirrored the present law in China. However, the bill was never introduced, a sign that it was not received well by other MOCs. Another bill of this nature has not been floated or introduced since this one was broached in 2016.
As discussed in greater detail in Chapter II, in the 1990s, the Clinton Administration attempted to ensure exceptional access by the government through the Clipper Chip. Leaders in the technology industry, privacy advocates, and MOCs met this move with heavy resistance. At the time, Representative Goodlatte strongly opposed the Clinton Administration’s initiative, and even introduced legislation in multiple congresses, “to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption.” At the time, he stated, “Strong encryption prevents crime. … [It] allows people to protect their digital communications and computer systems against criminal hackers and computer thieves.” It was shortly after this interview that the administration abandoned the idea of legislating on exceptional access. Goodlatte is still a MOC today and made additional comments in 2016 as the issue ramped up again. Goodlatte wrote a column for the media in which he opened with the statement that, “Encryption is a good thing,” and concludes that U.S. citizens rely on strong encryption, a position for which he appears to give unwavering support.

At the same time, it is clear that he and other MOCs believe that legislating the issue of encryption is Congress’ duty. In the same column referenced previously, Goodlatte states he believes Congress must find solutions for law enforcement instead of allowing courts to interpret laws that were not written with contemplation for encryption issues. He and ranking member Conyers formed a bipartisan encryption working group that made the following observations at the end of 2016:

- Any measure that weakens encryption works against the national interest.

---

334 Kehl, Wilson, and Bankston, *Doomed to Repeat History?*


338 Goodlatte.
• Encryption technology is a global technology that is widely and increasingly available around the world.

• The variety of stakeholders, technologies, and other factors create different and divergent challenges with respect to encryption and the “going dark” phenomenon, and therefore, no one-size-fits-all solution to the encryption challenge.

• Congress should foster cooperation between the law enforcement community and technology companies.339

Chairman McCaul of the House Homeland Security Committee and Vice Chairman Warner of the Select Committee on Intelligence introduced the Digital Security Commission Act of 2016 in the 114th Congress. An important part of this legislation would have established the McCaul-Warner Commission, a 16-member commission with the following stated purpose of:

bring[ing] together leading experts and practitioners from the technology sector, cryptography, law enforcement, intelligence, the privacy and civil liberties community, global commerce and economics, and the national security community to examine the intersection of security and digital security and communications technology in a systematic, holistic way, and determine the implications for national security, public safety, data security, privacy, innovation, and American competitiveness in the global marketplace.340

The bill garnered some support and it would have potentially brought the Congress closer to legislating on encryption, but it was never voted out of the House Committee on the Judiciary (HJC), chaired by Representative Goodlatte (whose stances on weakening encryption to assist the government were noted earlier in this section).


340 H.R. 4651.
Assessing the political climate of encryption, it appears that some in Congress are interested in legislating on the issue. However, based on the reception of the Feinstein-Burr proposal, not enough MOCs are interested in moving in the direction of exceptional access. Meanwhile, the observations of the Goodlatte-Conyers working group itself make no reference to legislating. This continued lack of congressional interest leads to the reasonable conclusion that China’s approach would not be politically acceptable.

b. Acceptance by the U.S. Population

Relative to the expected reception of the U.S. population, based on the previous analysis of politicians’ actions and inactions, it may be expected that congressional representatives are responding to U.S. citizens’ reluctance in allowing government access. However, an examination of polls relative to the issue at the time of the 2016 FBI v. Apple debate illustrates mixed reviews.

A Reuters/Ipsos poll taken contemporaneously to the Apple v. FBI debate, made the following observations:

- 46% agreed with Apple’s position [to resist the FBI’s requests and subsequent litigation] to unlock the [terrorist’s] phone, while 35% said they disagreed.

- 46% agreed when asked if the U.S. government should be able to look at data on Americans’ phones to protect against terror threats, while 42% said they disagreed.

- 69% said they would not give up email privacy even if it would help the government foil foreign terror plots and 75% said they would be unwilling to give up text-message privacy for the same reason.341

This poll had similar results to one conducted by the Wall Street Journal and NBC News:

- 47% said Apple should not cooperate with the government, 42% said they should.

- 47% said they feared the government wouldn’t go far enough [in monitoring terror suspects’ communications], while 44% feared the government would go too far [and violate the privacy of citizens].342

The Reuters/Ipsos and Wall Street Journal/NBC News polls lead people to believe that Americans want to keep their device data private. However, two other polls provided contradictory results.

The Pew Research Center conducted polling in the same time period, which provided the following data:

- 51% say Apple should unlock the iPhone to assist the FBI investigation, [while] 38% say Apple should not unlock the phone to ensure the security of its other users’ information.

- Among those who personally own an iPhone, 47% say Apple should comply with the FBI demand to unlock the phone, while 43% say they should not do this out of a concern that it could compromise the security of other users’ information.

---

Among those [who don’t personally own] an iPhone, 53% say Apple should unlock the phone, [while] 38% say they should not.\textsuperscript{343}

CBS News and the \textit{New York Times} also conducted their own poll, asking the question, “Should Apple create a way to unlock the iPhone of the San Bernardino shooter?”\textsuperscript{344}

- 50% said that Apple should unlock the phone...[and] 45% think [Apple] should not.

- More than eight in 10 Americans think it’s at least somewhat likely that if Apple creates a way to unlock the iPhone it will create a precedent for the future.

- Two-thirds think it’s at least somewhat likely it will make other iPhones more vulnerable to hackers.

- Two-thirds also think it’s at least somewhat likely that the [suspect’s] iPhone contains information that could help the government in its investigation.

- 26% think the federal government has gone too far in infringing on people’s privacy in the fight against terrorism, while the percentage who thinks the government hasn’t gone far enough has

\textsuperscript{343} According to interviewers at Princeton Data Source under the direction of Princeton Survey Research Associates International, the analysis in this report is based on telephone interviews conducted February 18–21, 2016 among a national sample of 1,002 adults, 18 years of age or older, living in the continental United States. “More Support for Justice Department than for Apple in Dispute over Unlocking iPhone,” Pew Research Center, February 22, 2016, http://www.people-press.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/.

risen. But 58% of Americans remain concerned about losing some of their privacy in the fight against terrorism.\textsuperscript{345}

The Pew Research Center and CBS News/\textit{New York Times} polls lead people to believe Americans may be prepared to accept the government obtaining exceptional access, at least in the case of a terror attack.

Based on the results of these four polls, overwhelming support does not appear to lean in one direction or the other on the issue of encryption, even in the context of a contemporaneous terror investigation. Given these mixed results, it is difficult to draw definitive conclusions as to where people may stand should a law be introduced that may compel decryption or assistance from private companies like Apple. It is reasonable to conclude that some people in this country may approve of the law while others may not.

4. Potential for Success

Using a similar framework for defining success discussed in the first section of this chapter, it is possible to evaluate the potential for success of China’s approach in the United States by looking at the approach’s impact on the encryption debate and its efficacy in obtaining decrypted device data.

\textit{a. The Encryption Debate}

The first criterion of success, whether the method employed resolves the privacy versus exceptional access debate, would not be met with the Chinese approach. The Chinese approach flies in the face of technologists and privacy advocates. This topic was covered in Chapter IV, and would not end the debate, but instead inflame it. Only those on the side of exceptional access would find satisfaction with this solution.

\textit{b. The Ability of Law Enforcement to Access Encrypted Information}

The second criterion, whether the method results in the ability of law enforcement to obtain usable data from a device that was once encrypted, is more straightforward. A law compelling companies or service providers to provide technical assistance or decrypt

\textsuperscript{345} CBS/\textit{New York Times} Poll.
data on a device is arguably the most effective solution to accessing encrypted data on a
device. As explained in the previous portions of this section, this approach raises
concerns about government overreach, could weaken the encryption products sold in the
United States, and could cause some companies to leave the United States; however, it
would likely be effective. The issue of effectiveness warrants a discussion on two fronts.

First, would such a law be effective in gaining the compliance of a company? There is no reason to believe that sending a court order to a company that compels them
to provide decrypted data or assistance in accessing that data would be any less effective
than sending a court order to an electronic mail provider requesting data from a user’s
account. Companies served with court orders have historically honored them knowing
that failure to do so could result in criminal contempt of court, with consequences of fines
and potentially incarceration for its executives. However, an exception does exist. Should
the developer of the encryption product be based outside of the United States, significant
difficulties could occur in pursuing legal means for assistance or decryption. The U.S.
government would be dependent on its legal attachés in U.S. embassies, its relationships
with local authorities, and mutual legal assistance treaties. The added layers of foreign
liaison work significantly complicate matters, and in some cases, make the possibility of
prosecution insurmountable.346

Second, would a company served with a court order be able to decrypt data or
offer technical assistance that would be effective in the pursuit of accessing otherwise
inaccessible information on a device utilizing encryption? The answer is, to some extent,
yes. Certainly in the Apple v. FBI case, the government believed Apple could force an
authorized update on the suspect’s phone’s operating system that would then allow the
government to attempt an uninterrupted number of passwords to access information on
the phone.347 Whether Apple developers have the ability to decrypt the data themselves

346 Kirby D. Behre, Lauren E. Briggerman, and Michael Anderson, DOJ Is Losing the Battle to

347 John L. Potapchuk, A Second Bite at the Apple: Federal Courts’ Authority to Compel Technical
Assistance to Government Agents in Accessing Encrypted Smartphone Data, under the All Writs Act
was never litigated; Apple claims that it does not have that capability.\textsuperscript{348} Since companies retain the source code of their operating systems and have intimate knowledge of the physical construction of the device, even if they do not have the capability to decrypt, they likely have the technical expertise to assist the government in gaining access.

C. FINDINGS

Using qualitative analysis to assess the markers of legality, cost, political acceptance, and potential for success of the approaches of Israel and China, it is possible to evaluate the approaches for application within the United States. The previous analysis yields the following core observations concerning the approaches of the two countries, which are summarized in Table 3:

- Relative to the structural approach of Israel, with its centralized forensic cybercrime unit and strong partnerships with the private sector and academia, legal barriers are unlikely; cost benefits are probable but likely; political acceptance is likely; potential for success is probable but likely.

- Relative to the legal framework instituted by China to compel technical assistance and decryption from telecommunications providers, legal barriers are likely; cost benefits are probable but unlikely; political acceptance is unlikely; potential for success is unlikely.

Table 3. Charted Representation of the Analysis of the Israeli and Chinese Approaches to Encryption Implemented in the United States

<table>
<thead>
<tr>
<th></th>
<th>Legally Acceptable</th>
<th>Cost Benefits</th>
<th>Political Acceptance</th>
<th>Potential for Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Israel</td>
<td>Yes</td>
<td>Probable (+)</td>
<td>Yes</td>
<td>Probable (+)</td>
</tr>
<tr>
<td>China</td>
<td>No</td>
<td>Probable (-)</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

The findings indicate that in an appraisal of each country’s approach, both opportunities and obstacles exist. In this search for a reasonable and effective solution for the United States, the obstacles for China’s approach appear to be in categories that would preclude its implementation in the United States. On the other hand, the obstacles in the Israeli approach are not insurmountable or reversible depending on a number of factors. The Israeli approach is a stronger, more viable solution for the United States than China’s approach.
VI. RECOMMENDATIONS AND CONCLUSION

The digital infrastructure is not always constructed with adequate regard for public safety, cybersecurity, and consumer privacy. Unless we overcome those complications, we will remain vulnerable.\(^{349}\)

—Deputy Attorney General Rod Rosenstein

This thesis set out to answer the question of whether the policy options of China or Israel offer models to address the issue of access to encrypted devices effectively and reasonably in the U.S. context. The basis of the question stems from a renewed debate over exceptional access to encrypted data that has churned for over two decades. This question has two underlying presumptions: a solution to this debate is needed and China or Israel offer models from which a solution can be derived.

The encryption debate manifests the ideological conflict that has occurred as a result of a migration to a technology-based society. Digital technology has permeated almost every facet of daily life, and electronic devices are driving this trend. In addition to lawful users, U.S. society has a criminal element in possession of devices used during the planning, execution, and aftermath of illicit activities. As a result, data and information residing on these devices have potential evidentiary value in a law enforcement investigation into these activities. At the same time, the encryption of this data is present, prevalent, and growing. This encryption is the flashpoint for the debate between those who favor exceptional access of encrypted data and those who are opposed to it.

Ironically, both groups in the dispute recognize the need for encryption, as well as the need for government access. However, the two are unable to reach a consensus on reasonably meeting both requirements, and from this point emerges the national debate. Too often that debate has entailed defending philosophical positions rather than finding

practical solutions. It is time the government moves on from a philosophical debate that has gained little ground in decades. The reality is that encrypted devices are being used to facilitate crimes like human trafficking, child exploitation, terrorism, and organized crime. The government has an ethical responsibility to prevent and investigate these illicit activities; policy-makers have an obligation to stop debating and act.

In evaluating the encryption approaches of other countries, this thesis sought to identify such a solution to guide U.S. policy. The selection of Israel and China was deliberate, as they offered particularly unique alternative models. Israel, a recognized world leader in cyber and security practices, was also notable for its lack of reporting within the country on an encryption debate. China, also a recognized world leader in cyber, had extensive reporting about the government’s precedent-setting decision to enact a counter-terrorism law that compels technical assistance and decryption from telecommunications operators and internet service providers. Given these characteristics, they fit the appearance of countries with models from which domestic policy guidance could be developed.

A. FINDINGS

Qualitative analysis was used to answer whether China or Israel offer a model to address the issue of access to encrypted devices effectively and reasonably in the United States. Examination of their primary approaches revealed a stark contrast between the two, with only Israel’s approach having viable characteristics for adoption in the United States. The respective policies of the two countries were evaluated in the context of their proposed application in the United States using the criteria of legality, cost, political acceptance, and potential for success.

The Chinese model, which resembles a legislative-based solution being proposed by the DOJ, the FBI, and others in favor of exceptional access, is not effective and reasonable based on these criteria. Attempts to implement the Chinese approach would be met with legal barriers, rejection by legislators and the American people, and it would have few cost benefits, if any at all. The policy would probably be successful in obtaining

350 Department of Justice, Statement of Christopher A. Wray.
encrypted information from electronic devices, but it would do nothing to end the encryption debate. It appears to be an unsatisfactory fit in almost every way with the one exception of gaining access to information on a device.

The Israeli approach satisfies many of the previously mentioned criteria and already resembles aspects of the decentralized approach the United States is taking towards dealing with encrypted data on devices. With its centralized forensic cybercrime unit and strong partnerships with the private sector and academia, the Israeli approach would not encounter legal barriers or political resistance in the United States. It would also likely be cost beneficial, especially to businesses with encryption equities. Although the potential for success in obtaining usable data from an encrypted device can only be evaluated as probable, if ultimately successful, it will put an end to the encryption debate. A U.S. approach tailored to be more consistent in structure with that of Israel has the potential to bring the United States closer to a viable domestic solution.

B. RECOMMENDATION

Based on the analysis of available information relative to the encryption approaches of Israel and China, this thesis recommends implementing a new initiative based on the Israeli model.

1. Conceptual Application of the Israeli Model

Mirroring the Israeli approach, this thesis recommends changes to the structural approach of U.S. law enforcement’s efforts to gain access to encrypted data on electronic devices through existing vulnerabilities. The fact that encryption is inherently vulnerable is a key takeaway from the initial chapters of this thesis, and Israel’s approach is best suited to take advantage of this weakness. Changes to U.S. law enforcement efforts include organizing its structure to be collectively and singularly focused on defeating device encryption, staffed with the appropriate personnel, and supported by adequate resources, all in collaboration with external partners.

Since it is not realistic for the United States to centralize law enforcement organizations, as they are in Israel, applying the Israeli approach in the United States
would mean developing a singular unit under the leadership of one agency tasked with coordinating the work of federal, state, and local partners. This approach would allow the U.S. cybercrime unit to have the traits of the unified Israel Police unit, including a centrally functioning coordination center and forensic laboratory under the control of that federal agency. Furthermore, given the greater size of the United States, smaller, regional forensic laboratories, under the control of the same agency, would mirror the placement of cyber officers around Israel, but on a greater scale. In addition to representatives from the governing agency, these smaller laboratories would be staffed with federal, state, and local forensic agents and officers. Ideally, these personnel would be trained under a shared curriculum and to a similar standard to ensure uniformity, validity, and reliability for the purposes of maintaining the forensic integrity of processes in the laboratories, especially as laboratories seek recognized accreditation.

Finally, the government will need to build stronger partnerships with private industry and academia. A multi-faceted approach by the government that includes direct communication and public outreach by the government will help to ensure this approach is implemented. Direct communication on the policy level would simply be continuing outreach like the Silicon Valley summit between private sector executives and Obama Administration officials that occurred in the summer of 2016, and with Trump Administration officials over the past year. In the view of one academic who has researched the encryption issue, a public relations and education campaign can be used to, “regain the public’s trust and to garner more cooperation and information-sharing support from private industry.”

Technology and cybersecurity companies can support many of the endeavors of law enforcement, and provide valuable knowledge and tools in the same way Cellebrite has for Israel. The alliances with academic institutions are arguably more valuable as a


352 Nguyen, “Lawful Hacking.”
human capital resource and a fountainhead of novel techniques from young, creative minds. University programs like MIT’s Computer Science and Artificial Intelligence Laboratory (CSAIL) and Stanford’s Applied Cryptography Group would be ideal candidates to approach for assistance. In academic settings, the talents of students can be identified, nurtured, and if possible, harnessed to assist law enforcement on technological issues relating to reasonable problems like extracting encrypted data from electronic devices believed to have been used during the commission of a crime.

Implementation of the Israeli model would result in creation of a U.S. cybercrime unit, more appropriately characterized as a unified forensic task force, singularly focused on device encryption. This unit would mirror the structural qualities of the Israeli cybercrime unit, its officers in the field, and its strong partnerships with academia and the private sector.

2. Considerations for the Practical Application of the Israeli Model

This proposed encryption solution in the United States calls for the traits identified in the Israeli cybercrime unit to be applied domestically. Given the size of the United States, this solution is likely to be best accomplished under federal leadership. A unit under the command of one entity in the United States, whether it is one law enforcement agency or a joint partnership of multiple federal agencies acting as one entity, would be best suited to mimic the unified approach of Israel successfully. A similar approach has already been achieved with counter-terrorism efforts of the FBI JTTFs under the National JTTF. Based on the extensive cyber forensic capabilities of the FBI and the Secret Service, the application of the Israeli model in the United States may be best suited under one of these agencies. It is also possible that a joint partnership of agencies may lead such a unit. Former Director Comey alluded to such an idea during a House Judiciary Committee hearing:

One of the things I’ve been trying to do is drive us closer together with the Secret Service because they have expertise...They’ve spent years developing that expertise, and so I don’t want to duplicate it, so we’re

353 Federal Bureau of Investigation, “What We Investigate”; Federal Bureau of Investigation, “Protecting America, National Task Force Wages War on Terror.”
trying to drive ourselves together. I’d like us to combine our task forces. It doesn’t make any sense for them to have an Electronic Crimes Task Force and me to have a Cyber Task Force, there ought to be one.\textsuperscript{354}

Nevertheless, considerations with both agencies, positive and negative, should be noted before further research is conducted to best determine the application of the Israeli model.

\textbf{a. The Federal Bureau of Investigation}

Some may readily conclude, based on their knowledge of the law enforcement structure in the United States, and the success of JTTFs, that a unified forensic unit should reside under the control of the FBI. Given the agency’s statutory authority, success with the JTTF program, and vast resources, the FBI certainly appears to have the aptitude to lead a forensic cybercrime unit and affiliated laboratories around the country. Before marching in that anticipated direction, elements about the application of the Israeli approach and the FBI should be discussed.

First, the Israeli approach may require the selected federal law enforcement entity that leads it to distance itself from intelligence agencies. Law enforcement agencies and intelligence organizations have distinct missions; the latter continues to come under public scrutiny for a myriad of reasons, many of them focused on government overreach and the sanctity of civil liberties like the right to privacy. The FBI’s two missions of domestic intelligence and criminal investigation are integrated, and are unlikely able to be satisfactorily separated. This situation could ultimately detract from efforts to build a national consensus on the issue of the novel approach or fail to attract those talented individuals outside of federal agencies with vital skills. This pool of potential assets who may want to assist would likely recognize the distinction of getting into a telephone of an alleged criminal or terrorist versus covert collection techniques used in domestic intelligence-gathering missions.

Secondly, the FBI already has similar programs to the Israeli approach in place. The agency administers the work of about 16 RCFLs in the United States through its

In addition, the FBI has a Going Dark program specifically focused on, “develop[ing] and acquir[ing] tools for electronic device analysis, cryptanalytic capability and forensic tools.” Based on the testimony of two of its most recent directors, and their concern over an unprecedented number of inaccessible encrypted devices in their possession, it would appear these efforts have not been fruitful in addressing the encryption issue. A closer look reveals inadequacies and room for improvement.

In addition to only operating about 16 RCFLs in the 50 states of the United States, with a broad focus on cyber forensics, the DOJ Office of Inspector General (OIG) conducted two audits of RCFLs in the past five years that raised a number of concerns. Generally, the DOJ OIG found the FBI reported 11 of the 16 RCFLs had backlogs of 10 or more unique items and, “the current process used to support the information found in the RCFL Annual Report is not adequate to ensure the accuracy of the information reported to Congress, FBI management, and the public.” The DOJ OIG concluded the RCFLs in New Jersey and Philadelphia both, “had mixed results in achieving [their] performance goals [and] material weaknesses in [their] Cell Phone Investigative Kiosk[s].” In New Jersey, the RCFL was found to have a material backlog of work and an inadequate process for training law enforcement. In Philadelphia, data reflecting “the number of law enforcement that were trained was inadequate, leaving the FBI unable to accurately determine the degree to which the RCFL program is accomplishing one of its core missions.” Participating agencies of the RCFLs reported being satisfied with

355 Regional Computer Forensic Laboratory, “National RCFL Program.”


359 Office of Inspector General, Audit of the Federal Bureau of Investigation’s New Jersey Regional Computer Forensic Laboratory, 14.

the work conducted at the RCFL but only consisted of eight agencies in New Jersey and six in Philadelphia, a minimal number when compared to the hundreds of law enforcement agencies operating within each state.\textsuperscript{361} Based on these reports, clear indications of performance, scale, and resource issues can be seen.

Similarly, the Going Dark program also appears to have scale and resource issues. Susan Landau draws a strong conclusion in her analysis of the program using the FBI fiscal year 2017 budget request as her source.\textsuperscript{362} She states:

\begin{quote}
The FBI has some excellent capabilities in cyber investigations, but not at the scale and level for solving today’s problems. The FBI’s Going Dark program, responsible for lawful hacking and technical challenges posed by encryption, anonymization, and the like, currently has 39 positions (11 agents) and a budget of $31 million; the 2017 budget requests an increase to $38.3 million but no additional positions. By comparison, the FBI’s physical surveillance effort has 549 agents and a $297.8 million budget. The inadequacy of the Going Dark effort may go a long way toward explaining the FBI’s current view of encrypted communications and secured devices.\textsuperscript{363}
\end{quote}

The contrast Landau draws to the physical surveillance program raises questions about the capacity of the FBI to adequately address an issue that agency and DOJ leaders have broached as a grave concern at multiple congressional hearings and public appearances. The focus of the program on encryption aside, the limited nature and resources of the program make it otherwise incomparable to the characteristics of the Israeli approach. The Going Dark program could be a key piece of any policy solution developed in the United States, but in its present form is insufficient.

While much of the previous discussion illustrates concerns about designating the FBI as the lead to an Israeli approach to encryption, it also highlights much of the infrastructure already in place should the FBI be tasked to pursue the policy recommendations of this thesis. As previously mentioned, the agency’s sizeable budget of almost $10B and record of success leading JTTFs make it an obvious candidate to head up device encryption task forces.

\begin{footnotesize}
\begin{enumerate}
\item Office of Inspector General, 10: Office of Inspector General, \textit{Audit of the Federal Bureau of Investigation’s New Jersey Regional Computer Forensic Laboratory}, 3.
\item Department of Justice, “Federal Bureau of Investigation.”
\item Landau, “The Real Security Issues of the iPhone Case,” 1399.
\end{enumerate}
\end{footnotesize}
b. The Secret Service

The noted limitations in current programs of the FBI present policy makers with an opportunity to look beyond the FBI before implementing an appropriately comparable solution resembling the Israeli approach. Consideration should also be given to other federal law enforcement agencies to lead this effort. Given the documented successes of the Secret Service in cybercrime, and the extensive amount of data forensically examined by its personnel, it is another agency worth considering.364

The Secret Service, an operational component agency of the DHS, is well positioned to establish a network of forensic laboratories consisting of a task force of public and private partners under its central authority focused on encrypted data extraction from electronic devices.

In 2001, the U.S. Congress passed H.R. 3162, the U.S.A. PATRIOT Act. Within that legislation was a section addressing U.S. Secret Service equities that stated:

SEC. 105. EXPANSION OF NATIONAL ELECTRONIC CRIME TASK FORCE INITIATIVE.

The Director of the United States Secret Service shall take appropriate actions to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.365

Since that time, the Secret Service established approximately 40 ECTFs around the country, each with a forensic lab in the field office from which the respective ECTFs operate.366 These task forces “leverage the combined resources of academia, the private

364 In FY 2016, the Secret Service was reported to have made over 250 cybercrime arrests preventing $558 million in potential loss and $125 million in actual loss. These arrests were in addition to the processing of 482 terabytes of data on 2,085 devices. See United States Secret Service, Presidential Campaign 2016: Annual Report (Washington, DC: United States Secret Service, 2016), https://www.secret service.gov/data/press/reports/USSS_FY2016AR.pdf.


366 United States Secret Service, “Investigation.”
sector, and local, state, and federal law enforcement.”

These partnerships are strong and have helped the Secret Service be successful in prosecutions in some of the largest data breaches in the country including TJ Maxx, Dave & Buster’s, and Heartland Payment Systems. The Secret Service has made remarkable partners in academia that have assisted them in investigations, including those with Massachusetts Institute of Technology’s Lincoln Laboratory, Carnegie Mellon University, and the University of Tulsa’s Tandy School of Computer Science.

The relationship the Secret Service has with the University of Tulsa is most relevant to this discussion, and could even serve as the template for other labs under the Secret Service around the country. According to one report:

The Secret Service has been running its Cell Phone Forensics Facility, a 10,000 sq. foot lab, in Tulsa, Okla., since 2008. Two Secret Service agents work there full time, aided by students and faculty at the University of Tulsa Cyber Corps Program. The facility trains federal agents in digital device forensics, invents its own hardware and software for parsing evidence from electronics, and uses that technology to examine 40 phones a year from police departments around the country.

Furthermore, the Secret Service is the only federal agency to operate a standalone cyber educational facility, the National Computer Forensic Institute, for state and local law enforcement investigators, prosecutors, and judges. At this academic institution, these individuals are taught, “how to conduct computer forensic examinations, respond to

367 United States Secret Service.


network intrusion incidents, and conduct cyber crimes investigations.”371 The school offers a four-week mobile device examiner and an additional advanced mobile device examiner course, which if harnessed properly, could serve to educate and train law enforcement staff for regional laboratories.372

The Secret Service is not without its own perceived limitations in leading the Israeli approach. Based on reports and testimony, these limitations stem from responsibilities and resources. The Secret Service has an integrated mission, whose responsibility includes protecting the President and others along with the financial infrastructure of the country. One congressional report argues that the two missions are distinct, and the investigations portion detracts from the agency’s need to focus on protecting its protectees.373 This argument is partially countered in the same report by testimony from former Deputy Attorney General (DAG) Mark Filip of a blue ribbon Protective Mission Panel when he is quoted as saying:

[T]here is certainly some benefits [sic] to be gained from the investigative mission to some extent. Now, there is a continuum in those investigative activities. To the extent, for example, that cyber investigations involve the safety of the First Family, of the President, that is probably going to be part of the core mission of the Secret Service.374

So, although the argument could be made for the Secret Service to be involved in a niche position to assist with device encryption since this help could always impact the protection of a president, former DAG Filip, like the House Committee on Oversight and Government Reform, believes that much of the agency’s cyber responsibilities may be


374 United States House of Representatives Committee on Oversight and Government Reform, 184.
better handled by other parts of the federal government while the agency focuses on protection.\textsuperscript{375} At the same time, the Secret Service is a resource driven agency, and all indications from testimony of the current director point to an ongoing need to reach healthier staffing levels and address attrition issues in the face of surveys indicating a morale issue among employees.\textsuperscript{376}

The negative issues arising from responsibilities and resources of the Secret Service should be taken in context. The positive aspects the agency has to offer with its ECTFs, cyber forensic laboratories, and partnerships are worth considering in assessing the practical application of the Israeli approach.

C. FUTURE RESEARCH

This thesis stops short of recommending which federal agency or agencies should lead this task force. Aside from the potential biases of the author, the practical application of the Israeli model is not within the scope of this body of work. The goal of this thesis was to evaluate the encryption approaches of China and Israel to determine whether either offers a model to address the issue of access effectively and reasonably to encrypted devices in the United States. The previous discussion considers two agency possibilities for the implementation of the Israeli approach to illustrate the idea that multiple options are possible within the United States to execute such a policy decision.

This thesis recommends that in identifying the leader for a device encryption task force, research should explore how the implementation of the Israeli approach by an agency would satisfy the criteria used for assessment referenced in the previous chapter. Some of the questions that could be asked include:

\textsuperscript{375} United States House of Representatives Committee on Oversight and Government Reform, 184.

From a legal perspective, how can an agency ensure satisfactory oversight of a group who will be trained to defeat encryption? How can the task force better educate prosecutors and judges to ensure the unconventional methods of the forensic examiners are understood and accepted?

In terms of cost, how can an agency best allocate funding in the implementation of this approach to achieve established goals? How will the rise of a public sector solution to device encryption influence the private sector in this field, and ultimately, affect current price rates for decryption services? How specifically will this approach increase cost efficiencies for both the government and the economy as a whole?

Relative to political acceptance, what practices can an agency rely upon to ensure that it sustains the support of political leaders and the U.S. public with this implementation? Will the implementation of a task force attract the attention of the U.S. Congress, and if so, what are the advantages and disadvantages to seeking statutory authorization eventually?

In discussing the potential for success, how can an agency recruit the best candidates away from their prestigious Silicon Valley and Cambridge jobs? How will an agency triage the devices submitted for decryption and data extraction to ensure they are able to maintain efficacy and satisfy the public they serve?

These questions are only a few that could be asked to better understand the practical implementation of this approach and the viability of a given agency to lead it. Further academic research is necessary to investigate fully the breadth of options for this approach in the United States.

Further research on certain aspects of the Israel and China case studies in this thesis could also add insight to implementation of the Israeli approach in the United States. The Israeli case study revealed a puzzle. Despite the high salience of security issues, Israel’s public and political leaders appear content with device encryption policies
as (or more) resistant to law enforcement than in the United States. Better understanding the sources of this satisfaction could help facilitate political acceptance in the United States. The China case study identified the difficulty of uncovering evidence that China has used its 2015 Counter-Terrorism Law to compel decryption assistance to support political or religious repression or human rights abuses. Discovery of such evidence would bolster the conclusion of this thesis that China’s model is inappropriate to the United States.

D. CONCLUSION

On Tuesday, October 10, 2017, Deputy Attorney General Rod Rosenstein delivered remarks on the issue of going dark to an attendance at the United States Naval Academy. As a proponent for exceptional access, he broached the idea of law enforcement access that had been left significantly dormant since Director Comey’s departure. He stated:

Such a proposal would not require every company to implement the same type of solution. The government need not require the use of a particular chip or algorithm, or require any particular key management technique or escrow. The law need not mandate any particular means in order to achieve the crucial end: when a court issues a search warrant or wiretap order to collect evidence of crime, the provider should be able to help.377

Within hours, the Electronic Frontier Foundation (EFF), a leading non-profit organization representing the civil libertarian views of technologists and privacy advocates alike published a point-by-point rebuttal.378 To Rosenstein’s previous point, the EFF states,

This is the new DOJ dodge. In the past, whenever the government tried to specify “secure” backdoored encryption solutions, researchers found security holes—for example, rather famously the Clipper Chip was broken quickly and thoroughly. So now, the government refuses to propose any specific technical solution, choosing to skate around the issue by simply

377 United States Department of Justice, “Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy.”

asking technologists to “nerd harder” until the magical dream of secure
golden keys is achieved.379

Two months later, FBI Director Christopher Wray, speaking in front of the House
Judiciary Committee, made a similar plea to that of Deputy Rosenstein, as the debate
over encryption continues with no apparent end in sight.380

Instead of making demands of communications providers and Congress that go
unanswered, it is time to chart a course that is more navigable. Based on the analysis of
two options being exercised by other countries, that trail has already been blazed by the
Israel Police cybercrime unit. This centralized, forensic effort that embraces partnerships
amongst government agencies along with the private sector and academia is a policy
solution that should be given serious consideration.

It is possible that at some point Congress will draft and pass legislation to address
the encryption issue. Since research for this thesis began, Australia and the United
Kingdom have indicated they would seek options to compel companies to disclose
plaintext of encrypted communications legally.381 In the United States, Congress could
undertake a similar course of action in a matter of days if so motivated, such as in the
wake of a ticking time bomb terrorist scenario gone badly.382 The sweeping surveillance
authorities granted under the PATRIOT Act less than two months after the 9/11 attacks
exemplify this prospect. However, waiting for such an event is morbid, defeatist, and
negligent with regards to the rising number of encrypted devices that law enforcement is

---

379 Kurt Opsahl, “Deputy Attorney General Rosenstein’s ‘Responsible Encryption’ Demand is Bad
and He Should Feel Bad,” Electronic Frontier Foundation, October 10, 2017, https://www.eff.org/deep

380 Department of Justice, Statement of Christopher A. Wray.

381 Jeremy Malcolm, “Australian PM Calls for End-to-End Encryption Ban, Says the Laws of
org/deeplinks/2017/07/australian-pm-calls-end-end-encryption-ban-says-laws-mathematics-dont-apply-
down; Investigatory Powers (Technical Capability) Regulations 2017, Draft Regulations (London:

382 The ticking time bomb scenario is a situation in which law enforcement captures a terrorist
suspected of having knowledge of the location of a bomb in a populated area with an imminent detonation.
In the case of encryption, the thought is that with a near-instantaneous solution of exceptional access,
authorities would be able to determine the location of the bomb and save lives. See “The Ticking Bomb
the-ticking-bomb-scenario.
unable to access. This reality underscores why the United States needs to act on a solution sooner rather than later.

In his statement cited above, Deputy Rosenstein also commented, “No solution will be perfect.” This thesis has noted a number of reasons why the Israeli approach would not be a perfect fit to the United States. It is also a solution however that could be amenable both to those in favor of exceptional access of encrypted data on devices and to those in opposition to it. It also lacks any need for statutory change to the laws as written. It will not work all of the time, and in some cases, the time it takes to access an encrypted device will be this approach’s worst enemy. However, history has shown that in every instance, even when proven to be perfectly secret, encryption is exploitable. Above all, this thesis contributes to a growing body of academic literature supporting a view that continuing a paralytic debate on the issue serves nobody’s interests. The onus is on those who hold absolutist positions in this debate to allow a reasonable and effective solution to be implemented in the United States.

---

383 United States Department of Justice, “Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy.”
LIST OF REFERENCES


Reuters. “Agree or Disagree with Apple’s Decision to Oppose a Court Order to Unlock a Smart Phone that Was Used by One of the Shooters in the San Bernardino Attack?” Accessed August 15, 2015. polling.reuters.com/#poll/TM853Y16/dates/20160220-20160223/type/overall.


INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California