THE CRYPTO WARS: INTERPRETING THE PRIVACY VERSUS NATIONAL SECURITY DEBATE FROM A STANDARDS PERSPECTIVE

A Thesis

submitted to the Faculty of the

Graduate School of Arts and Sciences

of Georgetown University

in partial fulfillment of the requirements for the

degree of

Master of Arts

in Communication, Culture and Technology

By

Sushovan Sircar, M.A

Washington, DC

April 20, 2017

THE CRYPTO WARS: AN INTERPRETATION OF THE PRIVACY VERSUS NATIONAL SECURITY DEBATE FROM A STANDARDS PERSPECTIVE

Sushovan Sircar, M.A

Thesis Advisor: Dr. Mark MacCarthy, Ph.D.

ABSTRACT

The Crypto Wars have emerged as an enduring policy stalemate between law enforcement and technology companies in the U.S for well over two decades. The battle for the control over encryption technology that has seen the two parties bitterly divided has been christened as the "crypto wars". This debate lies at the heart of the privacy versus national security debate in the U.S. While law enforcement and intelligence agencies have demanded access into encrypted communications in the interest of national security, the technology community has advocated for strong encryption to secure people's privacy rights. The National Security Agency's attempts at dictating communication encryption throughout the 1990s came to be regarded as Crypto Wars 1.0. The Federal Bureau of Investigation's complaints over "going dark" in 2011 which erupted in a public legal battle with Apple Inc. in 2016 is widely regarded as the second iteration of the same war or Crypto Wars 2.0.

As of 2017, this impasse has shown little signs of subsiding. Relatively few studies have studied the FBI vs. Apple controversy or the Crypto Wars as a standards issue. This thesis proffers a novel perspective by interpreting the Crypto Wars as a standards war and analyzing it through the framework of organizational field theory. Adopting a qualitative textual analysis method, it maps both the crypto wars along the same continuum as a contest to gain dominance over the encryption field by establishing winning standards. Through this framework the paper offers policy recommendations for a way forward in the future.

Acknowledgements

I would like express my sincere gratitude to the people who made this work possible. I am especially grateful to Dr. Mark MacCarthy, my thesis advisor, for not only guiding me through the arduous journey of the thesis but also igniting a deep interest in cyber issues of privacy, fairness and justice. Dr. D. Linda Garcia, who served as my second reader, has been a constant support during my time in Georgetown University. She has unlocked many doors of inquiry for me by intruding me to the world of standards and how they pervade very aspect of our lives and society. I am also thankful to Dr. Diana Owen and Sarah Twose, whose support during the thesis was invaluable and greatly elevated the quality of research.

I have been very fortunate to have had the love and support of my parents, Subhas and Sukhvinder Sircar, who made everything possible in the first place. I am grateful to Georgetown University for upholding the highest standards of education and resources through its Jesuit values and more than anything, making me a better person during my two years at this beautiful institution.

Table of Contents

Chapter 1: Introduction

On a Tuesday morning in February 2016, a judge in California issued a verdict in a court case that is part of an on-going struggle over the use of encryption technology christened as "Crypto Wars 2.0". Although the legal battle between two U.S. behemoths, fought largely in public over six weeks, ended without an outcome, it raised more questions than it answered in the process.

The suffix "2.0" suggests there was a "Crypto Wars 1.0" which preceded the incident of 2016. Indeed, a similar debate in the 1990s arose when the U.S. government advocated a backdoor in encrypted communication devices. The solution proffered by the government was a "Clipper Chip", a cryptographic chipset allowing law enforcement agencies to decrypt any traffic for surveillance purposes. This approach was consistent with the policy adopted by the United States Congress in passing the Communications Assistance for Law Enforcement Act (CALEA) in 1994, requiring communication carriers to engineer their facilities to provide for authorized real-time government wiretaps. However, extending this idea to all communications devices was abandoned in 2000.

The primary debate and the ensuing questions, however, have largely remained the same – the public's ability to use strong encryption and their right to privacy versus the government's ability to access communications in the interest of national security. The debate has resurfaced at regular intervals for nearly half a century since the 1970s in response to the advancement of technology and occurrences that threaten security.

The current debate, "Crypto Wars 2.0," intensified after the revelations in June 2013 that U.S. intelligence agencies had engaged in extensive monitoring of U.S. citizens on private communications networks. Technology companies reacted to these revelations with significant enhancements in encryption of information at rest in devices and in transit on their systems. Law enforcement and intelligence agencies complained that these increased security measures were hampering their efforts to detect and investigate criminal and terrorist activity.

In the aftermath of a mass shooting in San Bernadino, California, on December 2, 2015, the Federal Bureau of Investigation (FBI) recovered a phone of one of the gunmen and wanted Apple to help "unlock" it. When talks collapsed, a federal magistrate judge, at the U.S Department of Justice's (DOJ) request, ordered Apple Inc. to supply the FBI with a specialized software that would disable the in-built encryption and grant access to the investigating authorities. Apple, one of the most valuable technology companies in the U.S, found the ruling unacceptable, describing the government demand as one "that threatens the security of our customers". What followed over the next 42 days has been variously described as not only a battle between privacy and national security but also a battle between information security and national security. Apple's open letter in response to the court order stated, "But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone" (2016). The letter, signed by Apple CEO, Tim Cook, signaled a willingness to fight law enforcement on encryption standards.

On March 28, 2016, the federal prosecutors filed a motion to vacate the order as a private third-party emerged with an offer to help the FBI unlock the gunman's iPhone 5C. The sudden

and unexpected end to one of the most publicized legal battles thus fizzled out without setting a precedent for future cases of a similar nature.

An exploration of this recurring debate that once again presented itself in a new avatar points to a position of stalemate that has persisted well over two decades. The latest chapter of the debate in the form of the legal tussle between Apple and FBI did little to pave a way forward either in terms of a solution or cooperation between law enforcement and the communication technology industry.

However, a number of significant differences exist between the previous installment of the "war" and the latest one. Primarily, two major trends have redefined the landscape of the battle since the first crypto war ended in 2000. According to Jonathan Zittrain (2016), the first arises from the terrorist attacks of 9/11. "The attacks on the World Trade Center in New York reshaped the priorities of the U.S intelligence community, as extraordinary resources have been allocated to prevent and counter terrorism" (2016). The second trend is "the mainstreaming of the Internet and surrounding technologies built around and upon it, which has led to an unprecedented amount of data that can be analyzed by the intelligence services." (2016).

Indeed, these two events have reshaped the contours of the debate. The recent Crypto Wars 2.0 controversies and their culmination in the 2016 Apple-FBI court confrontation contains both elements. The fear of terrorist strikes on US soil has greatly intensified law enforcement's efforts in gathering intelligence to thwart activities that might pose a threat to the security of the nation. It is in this context that the terms "national security" assumed new meaning and significance in the debate. The rise of the internet as a mainstream communication channel has meant that millions of people now exchange information through the online route than two decades ago. Importantly, the emergence of smartphones, which technically are high speed

computers, means the mobile phone is now a valuable repository of information. For agencies like the FBI, the National Security Agency (NSA) and the Central Intelligence Agency (CIA), this also means that terrorists and suspected anti-US elements also use the same technologies to communicate. The latest phase of the debate was provoked by the San Bernadino shootout, which killed 14 people and injured 22.

Additionally, the interim debate since 9/11 has given rise to an entirely new vocabulary to both sides to argue their cases. Not only has "terrorism" entered the debate lexicon but several other phrases are also now common parlance. The Bureau started publicly raising concerns in 2011 about its ability to capture online communications. The FBI's then-General Counsel, Valerie Caproni, appeared before the Senate Judiciary Committee and used the phrase "going dark" to characterize the concern, citing "a widening gap between law enforcement's legal privilege to intercept electronic communications and its practical ability to actually intercept those communications" (Gasser et al., 2016). The phrase "going dark" was echoed by FBI director James Comey in 2015.

"Crypto Wars 2.0" therefore, can also be viewed as a part of this proliferating vocabulary that aims to capture and organize the evolution of this on-going debate. The importance of this renewed debate draws from this unique landscape in which it is now operating. Therefore, even though the core questions remain the same, the arguments for them have evolved. However, even at the end of the latest phase of the debate, the deadlock remains. This thesis will engage with the new nuances and argue that the second installment of the crypto war is a thematic continuation of the first that ended in 2000, and will examine them as such.

The central hypothesis of this paper is that the current stalemate between law enforcement and technology companies over data encryption arises from an acute standards

vacuum. The paper argues that the battle over encryption in communication devices is essentially a standards contest between law enforcement and technology companies. In particular, the paper seeks to find whether the standards that were established at the end of Crypto Wars 1.0 inform or impact the standards war in Crypto Wars 2.0. In other words, is there a standards link between the two Crypto Wars?

This leads us to the question about what "standards" precisely mean. "Standards are about the ways in which we order ourselves, other people, things, processes, numbers, and even language" (Busch, 2011). As "fundamental building blocks of society" they constitute an "agreed upon set of meanings, scripts, and rules guiding behaviors and governing relations". (Garcia, 2013). They prescribe "rules or protocols to be followed by individuals and organizations, as well as penalties in case of violation" (Hao, 2014). These definitions help to contextualize the privacy versus security debate by suggesting that law enforcement and technology companies lack a fundamental agreement of what the guiding rules or protocols should be. Standardization, therefore, offers a path towards coordination and cooperation by setting the rules of the game.

The thesis seeks to draw on the historical precedents with particular emphasis on the crypto war of the 1990s to analyze this current stalemate between law enforcement and technology enterprises, one that has continued to resurface in several other similar instances. The central aim of the research is to study the acute lack of consensus, which, the paper hypothesizes, arises from a vacuum in technical and policy standards to guide such issues. While policy standards refer to laws and regulations that outline a behavioral protocol, technical standards define the scope and nature of encryption. The paper will also explore attempts by both sides to unilaterally set standards.

In examining the hypothesis, two primary research questions arise.

What are the policy standards and technology standards vacuum?

i) **Policy standards vacuum:** This explores the relevant laws that govern the interaction of the two sides and whether they form an appropriate standard of coordination. From a law enforcement perspective, the question that arises is - should tech companies be required to engineer their systems, software and devices so as to be able to comply with law enforcement requests for access to information assuming they have satisfied appropriate legal processes?

ii) **Technical standards vacuum:** What should the standard of construction and encryption in devices be that both assists law enforcement as well as protect the privacy and security of its users?

"Standard setting is a complex process that cuts across micro, mezzo, and macro levels. To incorporate these levels into a unified approach, we need to adopt an organization field approach." (Garcia et al, 2013). In other words, by using organization fields as a framework of analysis, we can identify standards gaps and standard setting attempts by relating two distinct entities (FBI and Apple) within the same context.

According to Fligstein and McAdam (2012, p.83), an organizational field is characterized by the "ongoing internal tensions between incumbents and challengers in the contest for positioning." In the event of the organizational field becoming a battlefield among contesting actors, as we have seen between the FBI and Apple, the actors are likely to reach out (usually to the state) for external assistance. We saw this concept manifested by the actors battling it out in

the courts of California. With the legal situation still unclear, the parties have returned to the pre-court case status quo.

Therefore, a standards perspective of the stalemate using an organizational field theory framework enables us to locate the problem as a standards issue and offer possible solutions by coordination through both policy and technical standards. The research employs a multidisciplinary approach and explores the subject of information privacy and surveillance from a standards perspective. In doing so, the paper will contribute to two major fields - privacy studies within the cybersecurity domain and the domain of standards studies. A standards analysis of a decades old deadlock presents a unique perspective to a complex partisan issue. While the debate has merited extensive discussion and research, a standards analysis can provide a new approach and offer possible ways forward.

Chapter 2 lays down the theoretical framework to analyze the crypto wars. It achieves this by defining the key concepts of the paper and laying down the features of organizational field theory and the standards setting process. In chapter 3, the paper conceptualizes the privacy versus security debate by unpacking the existing literature on the 'crypto wars' of the 1990s and 2016. An important part of this chapter will also be the examination of relevant laws in this period related to the debate, particularly the Communications Assistance for Law Enforcement Act (CALEA), 1994. Bases on a critical overview of the literature on the debate, the paper will show how the current debate, dubbed "crypto wars 2.0," is thematically connected to the events of the preceding decades.

Chapter 4 and 5 identify and locate the two wars within an organizational field context and then proceeds to study those fields. The field interactions will be informed by a standards

contest and standards setting perspective. This chapter will provide insights into the relation among actors, their strategies and positioning for dominance as well as a link between the two crypto episodes.

Chapter 6 will lay down the detailed analysis based on the discussions in chapter 4 and 5. The analysis and findings will identify the specific areas where standards gridlocks exist and inform the policy recommendations. The following chapters will refer to the concepts and definitions posited in this chapter. In particular, concepts from standards setting and organizational field theory will inform the understanding of coordination and cooperation problems associated with the encryption debate.

Chapter 2: Theoretical Framework

2.1 Introduction

This study seeks to perform a standards analysis of the "Crypto Wars" with a focus on the recent "Crypto Wars 2.0", interpreting the FBI vs Apple battle as battle for standards dominance. In doing so the paper examines the larger privacy versus national security debate from a standards setting lens in order to identify the policy and technical gaps in the standards arena. It does so by exploring the first crypto wars of the 1990s so as to understand the encryption standards set by the NSA in telecommunications and the response of technology companies, cryptologists and privacy advocates. The insights of Crypto Wars 1.0 serve as a background to explore the new crypto war.

This chapter conceptualizes a standards framework for analyzing the two crypto wars. It builds upon our understanding of market standard setting mechanisms, network power and borrows its framework from organizational field theory. As such, the paper views standard setting as a complex, expensive and lengthy process that involves multiple stake-holders with varying objectives. This chapter lays down the major concepts of this research. It begins by defining the concepts of privacy, national security and encryption. It articulates the scope of privacy and security in the context of this debate and asks whether law enforcement authorities should have access to encrypted data with a lawful court order. The second half of the chapter discusses standards and proposes a standards-based theoretical framework. Based on this theoretical framing the chapter concludes by describing how a standards framework built upon organizational fields can reveal unique insights into a decades old debate.

2.2 Privacy

The FBI vs. Apple battle of 2016 was christened “Crypto Wars 2.0”, alluding to the key escrow and clipper chip controversies of the 1990s that were dubbed “Crypto Wars 1.0”. In both these “wars”, the larger debate revolved around a privacy versus national security tradeoff. While technology companies and scientists advocated for stronger commercial encryption and innovation that ensures greater privacy benefits for users, the NSA, which introduced the Clipper Chip and promoted the key escrow system in the 1990s, advocated for law enforcement access into communications systems for national security purposes.

Privacy has famously been described as ‘the right to be left alone” (Warren & Brandeis, 1890). Samuel Warren and Louis D. Brandeis’ 1890 essay “*The Right to Privacy*” set forth the tort of invasion of privacy. The essay advocated for the recognition of "the right to privacy, as a part of the more general right to the immunity of the person, - the right to one's personality” (1890). A right to privacy also meant that unjustifiable intrusions by the government on the privacy of the individual must be deemed a violation of the Fourth Amendment (Edgar, 2016).

This brings us to the Fourth Amendment to the US Constitution. The US privacy regime has a network of constitutional, common law and statutory law protections to regulate government access to information. The Fourth Amendment falls under the pillar of constitutional protection.

The Fourth Amendment reads:

> “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be

> violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Two issues crop up. *First*, the Fourth Amendment is only concerned with searches carried out by the government. *Second*, unless the government violates one's "reasonable expectation of privacy", no "search" has taken place. (Grimmelmann, 2016). The "reasonable expectation of privacy" test comes from *Katz vs United States* 389 U.S 347 (1967). Grimmelmann states that the Supreme Court found the bugging of a phone booth used by the defendant as a search by the police. Katz shifted the focus of the Fourth Amendment to "expectation[s] of privacy … that society is prepared to recognize as reasonable." Katz, 389 U.S. at 361 (Harlan, J., concurring).

A complication in the fourth amendment aligns with the same issue the FBI had raised in the San Bernadino case. A search by law enforcement is not considered "unreasonable" if carried out pursuant to a search warrant: a judicial order that gives law enforcement permission to carry out a search upon presentation of probable cause. In a statement before the House Judiciary Committee in July 2015, FBI director James Comey asked, "The core question is this: Once all of the requirements and safeguards of the laws and the Constitution have been met, are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime?" (2015)

Among the multiple sectoral statutes that protect information privacy from government access is the Electronic Communication Protection Act (ECPA) of 1986, which protects wire, oral and electronic communications while those communications are being made, are in transit,

and when they are stored in computers. The Act applies to email, telephone conversations, and data stored locally.

The Foreign Intelligence Surveillance Act of 1978 (FISA) is a federal law that describes procedures for the physical and electronic surveillance and collection of "foreign intelligence information" of "foreign powers" and "agents of foreign powers". If the target is a "U.S. person", there must exist probable cause to believe that the U.S. person's activities may involve espionage against the United States. It constitutes a violation of privacy for an individual to intercept another individual's communications and to use this information with the intent to harm. This weaves in information security as an aspect of privacy. It is important to note that there are no common legal protections against authorized government surveillance.

From a technology perspective, privacy has been described as "the ability to have a secure conversation" (Edgar, 2016). This is where encryption comes in as a tool to protect privacy. Ron Rivest, Adil Shamir and Leonard Adleman in their 1978 paper on public key cryptography stated that "encryption is the standard means of rendering a communication private (1978)". Timothy Edgar (2016) weighs in on this point by asserting that privacy according to technologists is the inability of an intruder to decipher the message. "That's what a technologist means when they think something is private. In other words, the system is either secure, in which case it's private-- Eve can't listen in on Alice and Bob-- or it's breakable, in which case it's not private" (2016).

2.3 National Security

The term "national security" in the context of this paper is used to refer to law enforcement's concern regarding access to communications for investigative purposes. The adoption of a technological architecture that inhibits the government's ability to access

communication even under circumstances that satisfy Fourth Amendment warrant requirements impedes investigations for national security purposes. This lack of access, which has been described as the "going dark" problem is, according to law enforcement agencies, a challenge to national security. In July 2015, FBI director, James Comey, in a statement before the House Judiciary Committee, articulated the relation between "going dark' and national security: "the growing challenges to public safety and national security that have eroded our ability to obtain electronic information and evidence pursuant to a court order or warrant. We in law enforcement often refer to this problem as "Going Dark" (2015)". Comey added that the harms resulting from the inability of companies to comply with court-ordered surveillance warrants are not abstract, and have very real consequences in different types of criminal and national security investigations.

At the height of the FBI vs Apple legal battle in 2016, both parties appeared at a Congressional hearing on Capitol Hill on March 1 where the same position was iterated once again in the opening statements and in Comey's testimony. Indeed, the hearing was titled "*The Encryption Tightrope: Balancing Americans' Security and Privacy.*"

The opening statements at the hearing before the Committee on Judiciary, House of Representatives, raised concerns for national security in the face of rapidly advancing encryption standards. "As encryption has increasingly become a ubiquitous technique to secure communications among consumers, industry, and governments, a national debate has arisen concerning the positive and negative implications for public safety and national security (2016)". The statement adds that law enforcement's sworn duty is to ensure that public safety and national security are not jeopardized if possible solutions exist within their control (2016).

Therefore, in the context of the FBI vs Apple case and the Crypto Wars, national security has been positioned as a competing value to the concept of privacy. The debate suggests a trade-off between the two where their relationship is inversely proportional - an increase in one is likely to lead to a decrease in the value of the other. While technology companies and privacy advocates argue for stronger encryption to increase user privacy, law enforcement bodies advocate for access to encrypted communication to ensure greater national security of US citizens.

2.4 Encryption

Having discussed the concepts of privacy and security in the scope of this paper and the debate we need to define "encryption" for the purposes of this paper. Here, the term encryption means the "conversion of plaintext into ciphertext using an algorithm to render the data unreadable without proper cipher and key to decrypt it." (Kehl et al., 2015) For the rest of this paper, all references to encryption will pertain to this definition.

The term cryptography refers to the "practice and study of theory and techniques for secure storage and communications". "Encryption is the actual process of combining the contents of a message ("plaintext") with a secret value or password (the encryption "key") in such a way that the content is scrambled into a totally new form ("ciphertext") that is unintelligible to unauthorized users. Only someone with the correct key can decrypt the information and convert it back into plaintext." (Kehl et al., 2015).

The privacy versus security debate revolves around the use and development of encryption. We will be examining encryption and its features in greater detail in the next chapter.

2.5 Standards

In this paper standards provide the basis for understanding, evaluating and analyzing the FBI vs Apple battle. A standards framework enables us to view the Crypto Wars and the privacy versus national security debate from a standards perspective, thereby allowing us to identify the policy and technical areas in which a standards vacuum exists. In other words, what standards are law enforcement and technology companies trying to set in the arena of encryption, and what standards need to be adhered to in order to achieve cooperation between the two parties entangled in a stalemate in order to reduce complexity and arrive at a path for coordination in the future?

We need to consider first what standards are. Standards have variously been described as "fundamental building blocks of society" (Busch, 2011). "In any given context, they constitute an agreed upon set of meanings, scripts, and rules for guiding behaviors and governing relations" (Garcia et al., 2005). According to Grewal (2008, p.22), "the standardization of measurement, language, laws, monetary system, formal education and production and transportation, not only reduced massive coordination failures but also allowed political, economic and cultural exchanges to extend beyond national and regional boundaries." In this sense, standardization presents a solution to issues of coordination and reciprocity in local and global systems. In the technological realm, "standards reduce transaction costs as well as add value to system components, allowing them to interconnect and interoperate in a transparent, seamless fashion" (United States Congress Office of Technology Assessment, 1992; 1994 cited in Garcia, 2005).

From the above descriptions it is easy to understand that standards, in any field of life, are ubiquitous and facilitate efficiency, cooperation and coordination. "Standards are about the ways in which we order ourselves, other people, things, processes, numbers, and even language"

(Busch, 2011). Garcia extends this idea to practical contexts by asserting that the kind of standards that are adopted have considerable import upon our daily lives. "Food and drugs must comply with health standards, cars use standards interchangeable parts: work places have safety standards; clothing come in standard sizes, workers perform standardized roles" (Garcia, 2015).

The definition of standards varies in different contexts, yet all embody certain common attributes. Bowker and Star (1999, as cited in Hao, 2014) offer six dimensions of standards:

1. Standards are the rules for production.
2. Standards reach across several communities of practice (be it temporally or persistently).
3. Standards are deployed to coordinate actors and things over distance and heterogeneous metrics.
4. Standards are usually enforced by legal bodies (be they professional organizations, manufacturers' organizations or the state).
5. There is no natural law that the best standards shall win.
6. Standards are subject to significant inertia and can be extremely expensive to change.

2.5.1 Key Standards Features

Simply put, standards are the rules of the game. "They are social and technical devices that support and facilitate interaction" (Busch, 2011). Standards, therefore, are of immense significance in the realm of business, industries and commerce as well. As Peter Grindley notes (1995), standards are central to business strategy. A company that succeeds in setting the standard for a technology, product or service can accrue massive social and financial benefits from having its chosen standard dominate the market. As Grindely says, "Being accepted as the common standard across an industry may be the single most important component of new

product success" (1995). Thus, standards have been vital in the successful integration of some of the most significant innovations of recent years, such as the video cassette recorder (VCR), compact disc (CD), and the personal computer (PC).

This discussion sets the tone for understanding standards setting in an open market.

Compatibility Standards:

Compatibility Standards depends on demand side-effects where the value of the product increases proportionally to the increase in its user base. A large installed base leads to greater production and makes the standard cumulatively more attractive to further potential users. "If a standard can establish a clear lead over competing standards it attracts increasing support and typically will sweep the market" (Grindley, 1995).

With respect to compatibility standards, firms have three strategic objectives (Grindley):

a. **To establish the standard in the market.** Ensuring whichever standard it chooses wins a standards contest.

The chances of winning a standards contest **depends on two positioning decisions**.

- Whether a company should develop a standard itself or adopt one from outside
- Whether a company should choose an open or proprietary standard.

Shapiro and Varian (1999) concur, stating that a firm intent upon gaining critical mass for its product must make a choice. The firm can either lobby its standard unilaterally and keep it proprietary with the hope that the market accepts it, or allow the standard to be open to competitors and have it accepted in the market.

b. To maximize the individual firms' profit from the standard.

With respect to this objective, it is important to understand that setting a standard involves a cost. Therefore, a standard that wins must bring profits to the winner of the standards contest. Garcia et. al (2005) warns of "collective action" dilemmas in this regard. In the context of organizations, failures occur when the dominant strategies pursued by individual actors lead to outcomes that are sub-optimal for the collectivity as a whole. Such situations are commonly referred to as 'social dilemmas' (2005). Two types of social dilemmas are found in the standard setting field.

- The problem of collective action associated with creating a public good.
- The second problem relates to common pool problems entailed in allocating and appropriating benefits. This is sometimes referred to in economics as a "prisoner's dilemma".

Moreover, these two dilemmas are interrelated and attempts to resolve one can exacerbate the other (Garcia et. al, 2005).

c. To compete effectively within an established market standard.

According to Varian & Shapiro (1999), "standards change competition for a market to competition within a market". The authors observe that participation in a formal standard-setting process, or assembling allies to promote a particular version of technology, typically involves competition *within* a standard.

Network Power:

"A network is an interconnected group of people linked to one another in a way that makes them capable of beneficial cooperation, which can take various forms, including the

exchange of goods and ideas" (Grewal, 2008). The same description applies to firms and technologies. Grewal observes that standards define the particular way in which a group of people is interconnected in a network. A standard must be shared among members of a network to the extent that they can achieve reciprocity, exchange or collective effort (2008).

In the context of networks, a standard gains value the more people adopt it. Such a product is said to exhibit *network externalities* or *network effects* (Grewal, 2008; Shapiro & Varian, 1999; Grindley, 1995). For many information technologies, consumers benefit from using a widely accepted format. Communication technologies such as telephones, e-mail, Internet access, fax machines and modems all exhibit network externalities (Shapiro &Varian, 1999). Hence it is essential to build a large installed base – a large number of users – quickly. As the installed base grows, more and more users find adoption of the technology worthwhile. This pattern of standards adoption results from *positive feedback*, a phenomenon that makes large networks grow larger.

Grindley (1995) reinforces this idea stating that the larger the installed base of users, the more complimentary products will be developed for the standard. A larger base with more complimentary support also increases the credibility of the standard. Together these events make the standard more attractive to new users. This brings in yet more adoptions, which further increases the size of the adoption.

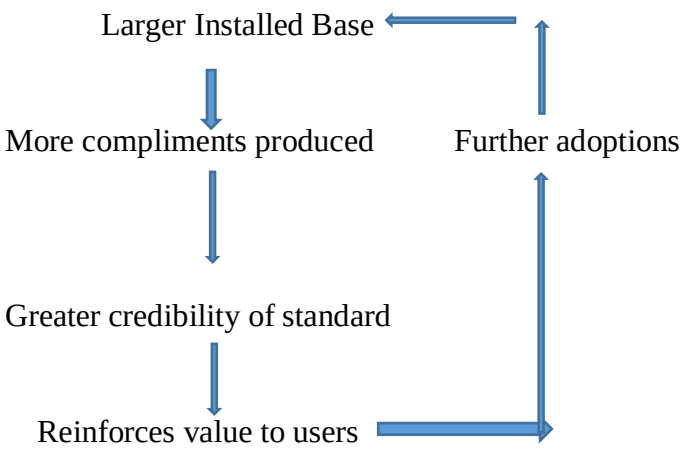

Fig 1.0 : Grindley's standards reinforcement mechanism

2.5 Organizational Field Theory

"An organizational field is the entire network of interdependent actors and organizations that, when considered together, comprise a recognized area of institutional life" (Powell & DiMaggio, 1991, Fligstein & McAdam 2012 as cited in Garcia, 2002). An organizational field perspective enables us to view all the actors as inhabitants of the same field, competing for dominance.

> "…[A] population of organizations operating in the same domain, as indicated by the similarity of their services or products. Included also are those others that critically influence their performance, including exchange partners, competitors, funding sources and regulators" (Scott, 2001).

Organizational fields are "highly contested arenas" (Garcia, 2004). In this paper, the arena is as a contest over standards. While a standards contest can be an expensive and lengthy affair, the winning standards promise benefits to the winner by enabling it to define the meaning and purpose of the field, the basis for coordination among actors and the relationships among them. This contested arena, according to Fligstein & McAdam (2012), is characterized by

ongoing internal tensions between "incumbents" and "challengers" in "the contest for positioning". Accordingly, fields rarely accept "taken for granted" reality and instead are characterized by "constant jockeying" within the field.

Having defined organizational fields, the actors within it and the interaction among them, we can consider the behavioral cycle of fields. Three stages can be observed in an organizational field – emergence, stability and reproduction, and rupture/crisis followed by reemergence and stability (Fligstein & McAdam, 2012). The stability of any field depends not only on how actors behave within the field by virtue of being embedded within a broad field environment, but also on the field's relation with other fields in its environment. (Fligstein &McAdam, 2012). Moreover, when a field experiences instability due to internal or external shocks, state or governmental intervention might be sought. Therefore, a field must take into account the activities of other fields and identify where it stands in relation to them within the broad environment.

2.6 Discussion

This chapter has provided the framework for capturing the relation and interaction among the actors in the privacy security debate, primarily law enforcement, the intelligence community and technology companies. The theoretical framework has two primary components that will enable us to analyze the encryption stalemate. *First*, the organizational field based framework allows us to identify and define the field within which the actors operate, position and interact to set the agenda for encryption in communication devices. By identifying the encryption field of action we can also identify other fields that affect the encryption field as well as capture the broad environment within which the field is nested. This structuring is important as it helps in

identifying not just actions within the field but also events in other fields and the external environment that have an impact on the field of interest.

Second, standards form the language of interaction between the actors within the encryption field. The interactions will be analyzed from a standard setting perspective and allow us to view the field as a contested arena where actors engage in a standards contest to claim dominance over the field and set the "rules of the game". Within the organizational field of *US Encryption Standards* the primary actors also represent distinct narratives. While law enforcement and intelligence communities seek to establish national security as the guiding motive behind encryption standards, technology companies contend that encryption standards need to be informed by principles of privacy.

In this thesis we analyze two case studies. The first is Crypto Wars 1.0, which unfolded in the 1990s and the second case study is the FBI vs Apple court controversy of 2016, which was dubbed Crypto Wars 2.0. An organizational field based theoretical framework allows is useful for two reasons. *First*, it provides a common denominator to examine both the events from a common analytical framework. *Second*, both cases involve multiplayer arenas where actors impact one another with their actions within and across the layers of the fields.

The next chapter examines the existing literature on the topic and lays out a detailed historical review of the events that were dubbed as Crypto Wars 1.0 and Crypto Wars 2.0. This will provide the information and background needed for chapters 4 and 5, which identify and locate the two wars within an organizational field context, allowing for their analysis The field interactions will be informed by a standards contest and standards setting perspective. These chapters will provide insights into the relation among actors, their strategies and positioning for dominance as well as a link between the two crypto episodes.

Chapter 6 will lay down the detailed analysis from the exploration in chapters 4 and 5. The analysis and findings will identify the areas where standards gridlocks exist and inform the policy recommendations.

Chapter 3: Literature Review

3.1 Introduction

This study unpacks the debate between privacy and national security from the perspective of both technology companies and the government. At the heart of this three-decade old debate lies encryption. The technology of encryption has led to a polarizing debate on a plethora of issues ranging from its usage and strength to regulation, accessibility and commerce, all of which have implications for privacy and security in the U.S.

By first defining the debate, this chapter explores the tussle between privacy and security and the resultant gridlock. It does so by examining the core arguments of the players from both the sides. In order to analyze the primary issues, the study offers an explanation of the concept and technology of encryption upon which the entire debate is predicated. It locates encryption within the precise context of the debate and looks at it from two perspectives: policy and technical. Having established the core parameters of the debate and introduced encryption within this context, the chapter proceeds to explore the first major clash between technology companies and law enforcement in the 1990s, which has been dubbed as "Crypto Wars 1.0". It summarizes and analyzes the nearly decade long controversy by outlining and reviewing the existing literature on the subject. The chapter then characterizes the Communication Assistance for Law Enforcement Act of 1994 and its role as a defining factor in the debate.

The second half of the perpetual tussle begins after the attacks of September 11, 2001. The terrorist attacks led to a renewed demand for greater access to intelligence gathering and also witnessed a steady strengthening of encryption technologies spurred by the growth of the Internet. The chapter explores issues of "going dark", the impact of the Edward Snowden

revelations and the eventual culmination into the publicly fought FBI vs Apple controversy. These issues collectively came to be known as Crypto Wars 2.0. By reviewing the literature on the first and second phases, the chapter synthesizes the evolution of the debate, lays down its main arguments, examines the perspectives of the government, the technology industry, encryption experts, advocacy groups and academia.

3.2 Privacy / Security Debate

The tussle between the government's law enforcement agencies and technology companies over communication encryption is not a new one. While both sides have made a renewed call to arms since 2010, which culminated in the publicly fought FBI vs Apple legal battle in February 2016, the first "shots" were fired back in 1992. Although the dispute had been brewing for years, the beginning of the Crypto Wars can be traced back to the Clinton administration's 1992 "Clipper Chip" proposal (Kehl et al., 2015). A closer reading of the background traces the origins of the debate back to 1970s with invention of "public key cryptography".

3.2.1 Key Features of the Debate

While the debate has evolved over four decades, the literature review reveals a commonality in the core arguments made by both sides that is yet to be resolved. The crux of the debate has often been summarized as one between the right to communicate privately by individuals and businesses and the need to access communication by the government for national security purposes. "The greatest dilemma arises from the fact that techniques that protect against illicit eavesdropping and data theft also threaten to prevent *licit* access to communications and data by law enforcement and intelligence agencies" (Froomkin, 1996). As framed in the media, encryption debates revolve around whether law enforcement should have surreptitious access to

data, or whether companies should be allowed to provide strong encryption to their customers at the expense of law enforcement's accessibility (Schneier, 2016).

Expanding upon this core dilemma, the primary arguments made by technology companies and privacy advocates on one hand and the government and its law enforcement bodies on the other reveal a number of consistent positions that both sides have held since the 1990s. Viewing encryption as a fundamental tool to secure their right to privacy, the technology industry and privacy groups have argued that encryption technology should be allowed to develop unrestricted. As they say, "Encryption secures our data and communications against eavesdroppers like criminals, foreign governments, and terrorists" (Schneier, 2016). The argument over encryption standards in communication devices and technology has verily been framed as one of privacy rights. Steven Levy, in his book *Crypto*, (2001) raises the question: "What if people themselves needed it [cryptography], to protect their communications and personal data from any and all intruders, including the government itself? Isn't everybody entitled to privacy" (2001; p.2). The two concepts – privacy and communications – were therefore stitched together as a single argumentative phrase. "Of course, what is of interest to us is communications privacy" (2011), writes Susan Landau in her book *Surveillance or Security*. Here the protections are the Fourth and Fifth Amendments to the constitution. These arguments make clear that advocates of privacy and encryption best practices are referring to privacy protections for two kinds of communication data - communication data in transit and data at rest.

On the government side, the primary arguments have mostly centered on "national security". This can be attributed to the fact that law enforcement and intelligence bodies like the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) have

spearheaded the debate on the government side, A review of the literature reveals three primary arguments on behalf of their position.

First, they argue that the growing use of encryption will "neutralize their investigative capabilities" (Abelson et al., 2015). Indeed, this argument forms the basis of the United States government's demand for limiting the growth and spread of encryption. This position has remained constant over the course of the two crypto wars and has served to shape their dominant policy regarding public communication encryption. The policy dilemma is especially acute in the United States because strong encryption can deny law enforcement agencies access to communications that it has enjoyed till the 1990s. In weighing the public's need for privacy and the government's need to provide security the government argued that, "important as confidentiality was for some public business, the government's need for wiretapping was more critical; widespread access to encryption would impede this" (Landau, 2011).

Second, in order to substantiate the first argument, law enforcement asserts that the encryption which grants privacy to individuals is a 'double-edged sword" as malicious actors will also hide behind the same technology to evade being apprehended. James Comey, FBI director, in a testimony before the United States Senate Judiciary Committee said, "these encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters" (2015). This claim has gained traction especially after a spate of attacks since 2015 which include garland, Texas (2015); Paris, France (2015); San Bernadino, California (2015), Brussels, Belgium (2016) and Orlando, Florida (2016). Terrorism suspects have often been suspected to be hiding behind widespread adoption of encryption technologies to mask their communications (Jaffer & Rosenthal, 2016).

Third, building on the two previous points, the government's third argument is more of a request before the judiciary. According to Comey, "we are asking to ensure that we can continue to obtain electronic information and evidence pursuant to the legal authority that Congress has provided to us to keep America safe" (2015). While the first two arguments have remained constant since the early 1990s, this argument emerged in 2010 and was amplified further during the FBI vs Apple court case in February 2016.

These arguments were first articulated in 2011 by FBI's then General Counsel, Valerie Caproni and have subsequently been described as the "**going dark**" problem.. Since then the phrase has been used repeatedly to characterize the government's concerns about the rapid advances in encryption technology. As Comey emphasized, the "going dark" problem is, at base, "one of technological choices and capability*"* (2015). He framed the issue as a question:

> "The core question is this: once all of the requirements and safeguards of the laws and the Constitution have been met, are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime?"
>
> - James Comey, 2015

3.3 Crypto Wars 1.0

Crypto Wars 2.0, which roughly began in 2011 was preceded nearly twenty years by Crypto Wars 1.0. The common thread that binds the two events is the encryption led privacy versus security debate, which lies at the center of the so-called wars. An Encryption Working Group report drawn up by the House Judiciary Committee & House Energy and Commerce Committee in 2016 drew attention to the FBI vs Apple case as a continuation of the of the first

debate in the early 1990s. This acknowledgement of the FBI vs Apple legal battle as thematically connected to the Key Escrow controversy has gained currency in the aftermath of the event. "With the benefit of historical hindsight a few years from now, we may look back on March 2016 as a turning point in the debate over encryption, surveillance and civil liberties" (Weitzner, 2016).

This paper examines the events from 1992 to 2000, commonly described as the "Clipper Chip controversy" or the "Key Escrow controversy". This paper argues that Crypto Wars 1.0 serves as a thematic precedent of the events of February and March 2016 when FBI and Apple entered into a heated legal battle over encryption standards. While the going dark issue and the court case have been referred to as "Crypto Wars 2.0", the events of the 1990s are referred to here as Crypto Wars 1.0 to establish the thematic similarities. This section examines literature related to the key events of the first Crypto Wars for purposes of comparison and analysis with respect to the second crypto wars.

3.3.1 1976 – 1992: Challenging Monopoly

Until 1976, only the military and intelligence communities employed encryption technology. The public had no access to encrypted communications as the technology remained closely guarded and restricted in use. As a result, despite academic research and interest in cryptography by the public, there was no concept of commercial or public crypto tools. In other words, the government had a monopoly over setting encryption standards. We shall explore this aspect in the next chapter.

This status quo changed in 1976 with the introduction of "public key cryptography" theorized by two researchers Whitfield Diffie and Martin Hellman. This theory was put into practice by mathematicians at Massachusetts Institute of Technology (MIT) who devised a split-

key encryption technique called RSA (Rivest, Shamir, Adelman – their last names). In 1991, computer scientist Philip Zimmerman released one of the first major practical tools for end-to-end encryption called Pretty Good Privacy (PGP). Zimmerman described the tool as helping individuals "take privacy into their own hands" (1991).

The proliferation of commercial encryption was interpreted by intelligence and military officials as a challenge to their monopoly. This commercial advancement represented an encroachment into what the NSA had "regarded as its birthright: the domination of cryptography" (Levy, 2001). As commercial applications grew in sophistication and accessibility "the full weight of the federal government was brought to bear to control the pattern and pace of their diffusion" (Kehl et al., 2015).

3.3.2 1993 – 1995: The Clipper Chip

By 1991, members of Congress had begun proposing draft legislations to ensure government access to plaintext of communication data. In 1992, discussions within the NSA began in earnest about a permanent solution to the "problem" of widespread encryption. (Levy, 2001, p228). On April 16, 1993, the White House officially adopted the Clipper Chip. A press statement referred to the Chip as a solution to the "problem of encryption as a double edged sword" while also acknowledging the "privacy of citizens". According to the statement the Clipper Chip was aimed "to provide law-abiding citizens with access to the encryption they need and prevent criminals from using it to hide their illegal activities". The statement therefore mentioned both privacy and security issues, thereby defining these concepts as tied to encryption. Also, it acknowledged the demand among civilians for encrypted communications.

The Clipper Chip was described by the government as a "state-of-the-art" microchip that offered superior encryption protection and contained a "master key" to give the government

access to encrypted communications by requiring copies of the keys to be held in escrow by trusted third parties (Abelson et al., 2016). This chip would be installed within landline telephones manufactured by AT&T and introduced as a voluntary standard. We shall examine the technical and policy standards of the Clipper Chip in the next chapter. The unique master-key in each chip was to be "split in two" and entrusted to the National Institute of Standards and Technology (NIST) and the Treasury Department.

In offering the public the Clipper Chip, the government dangled a carrot and a catch (Froomkin, 1996). The "carrot" was the Skipjack classified encryption algorithm, an eighty-bit key that was considered the strongest at that time. The "catch" was the government's ability to retain a copy of the master key that would give it access to messages exchanged using this chip (Froomkin, 1996).

3.3.3 1996 – 2000: Software Key Escrow

The Clipper Chip encountered dogged resistance from its inception and in 1996 was eventually abandoned in favor of a new strategy. Widespread opposition from technology companies, researchers, computer scientists and privacy advocates piled pressure on the government's attempt to abolish the Chip as a dominant standard. Diffie, the father of public-key cryptography argued that key escrow eliminated one of the system's key strengths: "it re-introduced reliance on third parties to protect the key" (Levy, 1994). The final death blow came in June 1994 from Matt Blaze, a computer scientist at AT&T Bell laboratories who in a paper revealed a serious flaw he had found in the Clipper Chip's security architecture, which could circumvent the interception capabilities put in place by the government.

By 1995, the government had "changed tactics" and shifted towards the concept of "software key escrow" also known as "commercial key escrow" and "key recovery schemes". As

the idea of having a physical chip baked into hardware and have government entities store parts of the key grew untenable, the tactic shifted to convincing companies to store keys themselves. "The plan contained performance criteria designed to limit applications to at best medium-quality ciphers and to ensure that keys would be accessible when the government presented a lawful request such as a subpoena" (Froomkin, 1996). This arrangement would continue to ensure that government enjoyed access to all encrypted communications.

This proposal, too, came under intense criticism from private industry and computer scientists. "Key recovery systems are inherently less secure, costlier, and more difficult to use than systems without a recovery feature. The complexity may well introduce unacceptable risks and costs" (Abelson, Anderson et al., 1997). The arguments against this new government tactic was not only criticized for its compromise of privacy but also witnessed growing criticism from a point of costs and economic nonviability.

3.3.4 2000: Export Restrictions Lifted

Strict government regulations of cryptographic tools resulted in their being classified as munition. This meant restrictions on export of encryption technology and algorithms. Prior to 1996, all products using encryption were controlled under the International Traffic in Arms Regulation (ITAR) and listed on the U.S Munitions List (USML). The U.S. government could not only monitor research and development of commercial tools but also indirectly influence their production by requiring companies to apply for an export (Kehl et al; 2015).

The rising costs for companies for having to design separate technologies for the same product within and beyond the U.S. led to a groundswell of opposition from the technology industry, which felt stifled in its ability to innovate. The regulations were seen as weakening the competitive edge of US products in a rapidly growing worldwide encryption market. A study by

the Economic Strategy Institute in 1998 estimated a loss between $35 billion and $95 billion over the next five years. A report by the Cyberspace Policy Institute at George Washington University in 1999 noted that there were over 500 foreign companies across 70 countries engaged in manufacturing and distributing cryptographic products. In January 2000, export restrictions were relaxed to make "unrestricted encryption source code" exportable.

3.4 Crypto Wars 2.0

The FBI vs Apple court case of 2016 that lasted for over 40 days marks the climax of a phase that has earned the epithet "Crypto Wars 2.0". The legal battle over a particular locked iPhone of a dead gunman quickly evolved into a debate about privacy and security of mobile phone users in general. Apple has contended that the court order could have grave consequences for privacy. The Justice Department has said Apple's inability to get into its own smartphones has "created a system tailor-made for criminals and harms national security" (New York Times, 2016). The Justice Department wanted to legally compel Apple to write software that would allow the government to try millions of random password combinations to get into the phone.

Broadly, the term "Crypto Wars 2.0" refers to five-year period from 2011 to 2016. The FBI has led the government's participation in the current debate (Gasser et al., 2016), which it ignited in 2011 with the phrase "going dark" to refer to the "potentially widening gap between our legal authority to intercept electronic communications pursuant to court order and our practical ability to actually intercept those communications" (Caproni, 2011). The phrase "going dark", which is now a part of the debate lexicon, has been adopted by law enforcement community to refer to the privacy versus security debate.

3.4.1 Apple vs FBI: The 42 Day War"

This section provides a comprehensive overview and background of the key features of the case.

Dec 2, 2015 – December 6, 2015: 14 people were killed and 22 injured in a shootout in San Bernadino, California on December 2. The gunmen were identified as a married US couple Syed Rizwan Farook and Tashfeen Malik. The FBI recovered Farook's iPhone 5C on December 3 and unable to access his locked iPhone without his passcode, FBI agents reached out to Apple on December 5. Apple complied with information to the FBI twice in response to requests. On December 6, FBI and San Bernardino County officials reset Farook's Apple ID password to access his iCloud backups but inadvertently ended up locking themselves out of the cloud. (Mashable, 2016)

February 16, 2016: A U.S. Magistrate for the Central District of California ordered Apple to assist the FBI in accessing Farook's iPhone 5C by creating a software that would circumvent its security features. The court wanted Apple to disable its auto-erase function that deletes all data after ten unsuccessful attempts.

February 17: Apple CEO Tim Cook responded to the court order by publishing a "Message to our Customers" (2016) where he laid down the main tenets of the company's position on the case. Describing the court's demand as setting a "dangerous precedent", Cook argued for strong encryption, warning that Apple users should "make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor." Strongly opposing FBI's position of the software being a "one time use" Cook warned of the risk of "sophisticated hackers" and "cybercriminals" exploiting the backdoor and put "digital security" and "privacy" of customers at risk.

February 19 – 25: Three days after a federal judge's order, the Justice Department filed a motion in court once again to compel Apple to assist with unlocking the phone. Describing Apple's refusal as a "marketing strategy", the Justice Department's brief stated that "Apple has responded by publicly repudiating that order." On February 25 Apple filed its first formal response since the court order. In a 65-page filing to vacate the order, Apple responded by dismissing the Justice Department and FBI's motion under the All Writs Act as inadequate and invoking the First and Fifth Amendments protections. Apple's court filing began by declaring that FBI's was seeking a "dangerous power" to "force companies like Apple to undermine its security and privacy interests of hundreds and millions of people around the globe" (2016, p.1).

February 29: In a separate but related case, a New York judge ruled in favor of Apple and denied a government request to compel the company to unlock a phone related to a Brooklyn drug case. The court's rejection of the All Writs Act was seen as a "useful victory" for Apple as the same statute had also been applied by the FBI in the California case and one that gives Apple's "pro-privacy stance a boost" (New York Times, 2016).

March 1: The action shifts to Capitol Hill as FBI and Apple trade blows before Congress. At a House Judiciary Committee hearing, FBI director James Comey admits to a "mistake made in the 24 hours after the attack" in reference to the resetting of Farook's iCloud password that locked them out of his phone's data. Apple reiterates its point regarding privacy compromise with Bruce Sewell, Apple general counsel, arguing that the FBI demand would "set a dangerous precedent for government intrusion on the privacy and safety of its citizens" (New York Times, 2016). The privacy position is supported by Republican Representative Jason Chaffetz who asked "how much privacy are we going to give up in the name of security," (2016).

March 3: Around 40 technology companies including giants like Facebook, Google, Microsoft and LinkedIn filed amicus briefs in support of Apple and against the government's demands in the case. The industry argues that its interests are aligned and raises "privacy rights of consumers in general" concerns against what they describe as "government overreach".

March 10 - 15: FBI and Apple "turn up the volume on the iPhone privacy fight" (New York Times, 2016) as the Justice Department files a point-by-point rebuttal to the motion filed by Apple on February 25. The Justice Department response said Apple and its supporters "try to alarm the court by invoking bigger debates over privacy and national security" (2016). On March 15, Apple filed its second and final response to the court before a crucial hearing of the case on March 22. Apple tries to refocus attention on the case as a fight over civil liberties and data privacy. "The issue cannot be weighed without taking into account the larger national debate over data privacy concerns", Apple stated. (2016).

March 21: An unexpected twist as FBI says it may not need Apple's assistance after all in breaking into Farook's iPhone. Fewer than 24 hours before the scheduled hearing, the U.S. Department of Justice asks to postpone the hearing, revealing that an "outside party" came forward at the last minute with a technique that could help the FBI get into Farook's iPhone without Apple's help (Mashable, 2016). The Justice Department seeks to vacate the order and says it will file a status report by April 5. The court case comes to a halt without a verdict.

March 28: The Justice Department declares that FBI had found a new technique to unlock the phone without help from Apple, allowing the agency to withdraw its legal effort to compel the company's assistance. A two-paragraph filing read it had "now successfully accessed the data stored on Farook's iPhone and therefore no longer requires the assistance from Apple." The American Civil Liberties Union says unlocking of the iPhone "doesn't mean the fight is over" as

it found 63 cases in which the government applied for All Writs Act orders to force Apple or Google to help access data stored on a mobile device, showing that while the San Bernardino case may have focused on an individual phone, the legal issues at stake may affect many more.

3.5 Discussion

The FBI vs Apple legal fight emerged as a "privacy versus security" debate as the case progressed over the course of 42 days. While Apple had raised the issue of privacy on the same day as the order was first passed on February 16, it was joined by over 40 companies and several academics, computer scientists and advocacy groups in the following days , who echoed Apple's privacy arguments. This effectively elevated the case into a larger debate over privacy rights as an entirely industry or technology companies rallied behind the case of privacy protection.

The Department of Justice and the FBI have maintained throughout the duration of the case that it sought access into Farook's phone in the interest of national security. Therefore, Apple must be compelled to comply with a legal court order for assistance after the FBI has satisfied the due process of the courts. The FBI has also acknowledged the issue of privacy in its legal briefings and testimonies by director James Comey. He wrote in a statement that the San Bernadino case "does highlight that we have awesome new technology that creates a serious tension between two values we all treasure—privacy and safety" (Lawfare, 2016).

The arguments from both the parties along with those of the technology industry, the government, press, academia and advocacy groups framed the 42-day long court battle as one of privacy and security.

A number of papers have been published since the case folded on March 28. Various departments of the government, academia, think tanks, journals and computer scientists have

written about the case as a privacy versus security issue. To that end, they have provided analysis, research and proffered various solutions, recommendations and opinions. However, while there exists an extensive body of research on the going dark issue, encryption and privacy between 2010 and 2016, research on the FBI vs Apple case using a standards perspective remains limited.

A team of experts led by Urs Gasser observed in their paper, "*Don't Panic*" (published before the court battle started), that the debate over encryption "raises difficult questions about security and privacy" (2016). While the paper concludes that the term "going dark" does not fully describe the future of government's access capabilities it observes that, from the national security perspective, it needs to be asked whether exceptional access would also increase vulnerability to cyber espionage. From the civil liberties perspective, the question raised is whether preventing the government from gaining access under circumstances that meet fourth Amendment standards strike the right balance between privacy and security (Gasser et al., 2016)

Jamil Jaffer and Daniel Rosenthal, professors of law with previous experience in the government, acknowledge the stalemate in the debate in their policy paper, "*Decrypting our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge*" (2016). "As a result of the overheated rhetoric on both sides, the nation now finds itself in the throes of a dangerous stalemate." (Jaffer and Rosenthal, 2016). The paper offers thirteen proposals to the current stalemate while opining that the "absolutism and polarization" in the arguments of both sides suggests an inflexibility and inability to reach an outcome (2016).

The privacy and security challenge is also examined in a paper by the American Enterprise Institute that looks into the FBI vs Apple case as a crucial chapter in the Crypto debate. The paper titled, "*Surveillance Versus Privacy, with International Companies Caught in*

Between" observes that the confrontation between Apple and the FBI is "today's most prominent case of a company torn in conflicting directions, representing a mix of several distinctive strands of conflict involving surveillance versus protection of privacy" (Horan, 2016). In analyzing the merits of the debate from the perspective of encryption the author asks whether it is possible to design encryption systems weak enough to allow official surveillance without also exposing it to terrorists and criminals. "What is the appropriate balance therefore between individual privacy and government surveillance in a dangerous world?" (2016).

This sentiment is echoed by Castro and McQuinn who observe that "some law enforcement agencies have renewed the debate about privacy, security and the rule of law in the digital age" (2016). Acknowledging in their paper that the debate surrounding encryption has created "one of the most enduring policy dilemmas of the digital age", one in which "there is no way to square the circle, so any choice will come with tradeoffs" (Castro & McQuinn, 2016). This paper also explores the developments of the first Crypto Wars and looks at the current FBI vs Apple debate as one of privacy and security with regards to encryption.

A year-end report published by the Encryption Working Group (House Judiciary & House Energy and Commerce Committee) also looks into the FBI vs Apple litigation. Analyzing the debate from an encryption perspective, the report does acknowledge the privacy aspects of the issue and proceeds to pose a number of questions that could take the stalemate towards a solution. In addition to privacy, the report also mentions "data security" in the context of privacy. "The increasing use of encryption can be attributed, at least in part, to heightened consumer awareness and interest in online privacy and data security" (Upton et al., 2016). Among the questions raised are "should the federal government take additional steps to address

greater security around private data?" and "how would consumers' privacy and data security suffer if encryption were weakened?"

Chapter 4: Standards Contest in the Crypto Field - Crypto Wars 1.0

4.1 Introduction

This chapter conceptualizes the stalemate between law enforcement and the technology community from an organizational field perspective. It locates the actors as inhabitants of the same field who are vying for dominance in order to set 'the rules of the game', define the space and the relationship among the actors in the field. The previous chapter has laid down the theoretical framework, which looks at the privacy versus national security debate surrounding encryption as a standards contest within an organizational field. The fields are "highly contested arenas" (Garcia 2013) characterized by "ongoing internal tension between incumbents and challengers" (Fligstein & McAdam).

An analysis of the interaction among the actors from a standards perspective will enable us to interpret their jockeying for dominance as a standards contest. Standards as the "fundamental building blocks of society" (Garcia, 2013) facilitate smooth interaction among actors and enhances coordination and efficiency in production. An actor who wins a standards contest dominates the field by defining its rules. We will be employing a market based compatibility standards approach, which, as Grindley (1995) posits, depends primarily on demand side-effects where the value of the product increases proportionally to the increase in its user base. A large installed base leads to greater production and makes the standard cumulatively more attractive to further potential users. "If a standard can establish a clear lead over competing standards it attracts increasing support and typically will sweep the market" (Grindley, 1995). In

this context actors have three strategic objectives: To win a standards contest and establish a standard, to maximize profits from the standard and continue to compete within the established standard.

In this chapter we will be analyzing Crypto Wars 1.0 that unfolded in the 1990s. The primary actors in this case are the National Security Agency (NSA), technology companies, cryptography scientists and experts, and the government. An organizational field based theoretical framework allows us to carry out the analysis for two reasons. First, it provides a common denominator to examine both the "wars" from a common analytical framework. Second, both cases involve multiplayer arenas where actors impact one another with their actions within an across the layers of the field. To frame these periods, the chapter draws on the literature of organizational fields (Fligstein and McAdam, 2012; Garcia 2013). The conceptualization provides a common framework for analyzing each episode of the crypto wars.

4.2 Crypto Wars 1.0

Encryption technology in the U.S. is not an invention of the computer era and traces its roots to as early as the 1790s when Thomas Jefferson, while serving as George Washington's Secretary of State, is said to have relied upon an encryption device known as the wheel cipher to send letters. (Kehl et al., 2015) For a majority of the twentieth century, cryptography and encryption techniques were used almost exclusively by members of the government, military and intelligence communities. Even after a market for commercial encryption took shape in the 1980s, until 1996 all crypto products were listed on the US Munitions List (USML) and placed under the strict control of the International Traffic in Arms Regulation (ITAR). Additionally, the government had placed strong restrictions on the export of encryption beyond its borders. Therefore, the intelligence and military enjoyed a monopoly over the use of encryption to protect

their documents and communications. It is important to note that prior to the 1980s encryption as a technology had little commercial market value and hence saw no attempts at mass production of cryptographic tools.

4.2.1 Early Signs of Field Formation: Challengers and Incumbents

The intelligence and military's monopoly over encryption suffered its first blow in 1976 when two researchers, Whitfield Diffie and Martin Hellman, published a paper on a new technology called "public key cryptography" which theoretically demonstrated a way for the public to communicate securely (Kehl et al., 2015). Within a year of Diffie and Hellman's "*New Directions in Cryptography*", three researchers at Massachusetts Institute of technology (MIT) put the encryption theory into practice. The technology created in 1977 knows as "RSA" (Initial of their names – Rivest, Shamir and Adleman) ensured a method of keeping communications private.

From an organizational field perspective, these developments provided the early signs of the formation of a field that challenged the monopoly of the incumbent intelligence bodies. Encryption had made its first appearance in the public domain and presented a challenge to the intelligence and military's proprietorship over the technology. The commercial viability of the technology, however, remained unclear in the early 1980s. Spurred by the growing adoption of PCs by individuals and businesses, an increasing amount of confidential data found its way into computers. This computerization of data led to an explosion in commercial demand for encryption in the mid-1980s. A new hitherto non-existent market emerged for secure communication and data protection technologies, rendering encryption a commercially viable product. By the advent of the 1990s encryption had considerable market value.

Thus emerged a field with the NSA as incumbents and technology companies as challengers to a common technology. The commercial development of cryptographic technology was driven both by corporations as well as computer scientists. While companies like Lotus Corporation's products warranted built-in encryption, Philip Zimmermann, a computer scientist designed one of the first major practical tool called Pretty Good Protection (PGP) for end-to-end public key encryption of files and emails in 1991 (Kehl et al., 2015). The early 1990s also witnessed the proliferation of mobile phones and the rise of the Internet. Matt Blaze, a computer scientist who later become a key figure in the first Crypto War, observed that information technology was getting "inexorably faster, cheaper and better, with the notable exception of security, which seemed actually to get worse with every iteration of Moore's law" (2011).

Therefore, by the early 1990s an explosion in demand spawned a market for encryption tools and products that rallied corporations and computer scientists towards meeting this demand. The early signs of coordination and development among market facing companies caused them to emerge as actors, specifically as challengers, and set in motion the formation of the crypto field. Cryptography would soon cease to be merely the esoteric realm of spies, armies, and governments, but would become "an integral part of the public information economy" (Blaze, 2011).

4.2.2 The 1990s: Contesting Standards in the Field

Prior to entering a standards analysis between the incumbent and challenging actors, it is important to examine the motivation of the actors within the field. The incumbent actors are the military and intelligence communities. They are identified as the incumbents because prior to the emergence of the field they held a monopoly over the technology. Even after the appearance of new actors who contest the terrain, existing regulations and rules ensured that the "rules of the

game" favored their grip over the field. Indeed, as the theory suggests, the incumbents define the space and meaning of the field and by doing so stamp their domination. The challengers in this arena are the technology companies and scientists who have devised public cryptographic tools that could potentially alter the nature of the field. As stated by Garcia (2013), they [challengers] "must not simply compete for resources but reinterpret current practices in the light of an alternate institutional logic".

This brings us to the question of motivation. It is important to note that the actors have different motivations for controlling the contested terrain despite battling over the same technology. The motivation of the incumbents is to define encryption standards in order to retain their privilege of access to communications of the public. The challengers, on the other hand, view encryption as a high-demand commercial good with a great market value. While incumbents wanted to hold on to their domestic monopoly and right to access communications, the challengers sought to invest in the technology in the hope of securing profitable returns. The incumbents did not display a commercial interest in profiting from the technology and hence did not adopt the competition route in order to defeat the challengers.

Although the intelligence community and technology companies have disparate motivations in controlling the field, they are compelled to take each other's actions into account in their behavior (Fligstein & McAdam, 2012). This was first observed in 1992 when telecommunication company AT&T announced a voice encryption device that could encrypt telephone conversations. Blaze, who was an employee of the company at the time states "when the US government learned of AT&T's plans to market the TSD, it worried that criminals might use the devices to thwart wiretaps (2011)."

4.2.3 Key Escrow and Clipper Chip: A Standards Contest Begins

As the field took shape and the actors emerged, a standards contest ensued. It is during this phase that the NSA attempted to wrest control over the encryption field and establish itself as the incumbent. We identify this field as the *US Commercial Hardware Encryption Field*. The broad encryption field can be divided into commercial and non-commercial encryption fields with intelligence agencies finding themselves faced with the prospect of being confined to the non-commercial sub-field. The 1990s witnessed a commercial encryption field carve out a space for itself that was hitherto non-existent. This chapter explores the NSA's attempt to dominate the commercial field. Additionally, the *US Commercial Hardware Encryption Field* witnessed a growing community of mathematicians, crypto researchers and privacy advocates enter the field. They are considered actors in the field as their actions are taken into account in the behavior of other actors.

In 1992, AT&T announced the TSD-3600D, a voice encryption device that could be installed in any standard wireline telephone (between the phone base and the handset). Calls placed to other TSD-3600D-equipped telephones would be automatically digitized and encrypted using the Data Encryption Standard (DES). With DES as its encryption standard, AT&T had planned to compete in the rapidly growing commercial crypto products market. The telecommunication giant was looking to set the TSD-3600 as the *de facto* standard by creating a large installed base of users who would communicate using the voice encryption device.

The NSA, perhaps, realizing that the standard that dominates the commercial sub-field would, in turn, attempt to challenge the larger US encryption field with its own standards. It is in this context that we can posit that the rise of a market for commercial crypto products where encryption devices had a high monetary value was of considerable concern for the NSA. It would

not only undermine its dominance over the field but could also independently deploy encryption standards that could prevent access to intelligence agencies.

Therefore, despite not being a part of the Commercial Encryption sub-field, the NSA led intelligence community tried to enforce a standard for the commercial sub-field that would suit its needs. It went about doing this by dangling carrots before AT&T and using government imposed regulations to stifle standards innovation in the commercial sub-field in order impose its standard. "When the US government learned of AT&T's plans to market the TSD, it worried that criminals might use the devices to thwart wiretaps" (Blaze, 2011). The NSA, instead, proposed a new escrowed encryption device – with a wiretap backdoor – and persuaded AT&T to replace the DES-based encryption scheme with a new system designed by the NSA.

Faced with a challenge from a new standard, Varian & Shapiro (1999) state that an incumbent has three choices:

i. Incumbent can deny backward compatibility to would-be entrant in the hope of blockading the entry of the new technology altogether, thereby extending the life of its own technology.
ii. Incumbent can rush to introduce its own new generation of equipment in order to win a standards war.
iii. Incumbent can ally itself with a new technology, hoping to benefit from its established name and an expanded market.

The NSA opted for the second option and also added an element of the third. It chose to draw up its own encryption standard for telephone conversations in the form of the Clipper Chip, which used the "Skipjack" algorithm. However, it would install the chip in the AT&T manufactured TSD-3600 and have it market it commercially. By doing so, despite not having a commercial

stake or profit motive in a market driven field, the NSA hoped to have its standard imposed and adopted by the market.

4.3 Unpacking the Standards Contest

The Clipper Chip standard that the NSA proposed to AT&T had two aspects.

i. It's "Skipjack" algorithm would provide stronger encryption than DES. The Skipjack algorithm within the Clipper Chip contained an 80-bit key as opposed to DES' 56-bit key. This would make it much harder to crack the Skipjack encryption compared to DES.

ii. The Clipper Chip would contain a backdoor to allow law enforcement access to plaintext communication. The keys of every conversation would be held in escrow by the Commerce Department's National Institute of Standards and Technology (NIST) and the Treasury Department.

The Skipjack algorithm infused Clipper Chip functioned like other strong crypto chips but with a difference: "a copy of the current session key, itself encrypted with a key known to the government was sent at the beginning of every encrypted communication" (Blaze, 2011).

Based on our framework, compatibility standards depend on demand side-effects, which make the core product more valuable the more users it has. "If a standard can establish a clear lead over competing standards it attracts increasing support and typically will sweep the market" (Grindley, 1995).

In this context of our framework, a firm has three strategic objectives. *First*, **to establish the standard in the market.** This means ensuring whichever standard it chooses wins a standards contest.

The chances of winning a standards contest **depends on two positioning decisions**.

- Whether to develop a standard itself or adopt one from outside
- Whether to choose an open or proprietary standard.

AT&T's first objective was, therefore, to ensure that whichever encryption standard it went with did end up becoming the market standard. From the telephone company's perspective, it had reasons to believe that the Clipper Chip could become the de facto standard. Given that the intelligence agencies had maintained their dominant incumbent position within the field because of strong government regulations that tilted the field heavily in their favor, the phone company believed that any standard that the government adopts as its policy would surely win a standards contest. To get AT&T on board, the government dangled three carrots before the company that were "too juicy to turn down" (Levy, 2001). *First*, AT&T could claim that it was actually providing a stronger level of encryption, since Skipjack was much more difficult to penetrate than DES. *Second*, the United States government would allow the encryption devices to be exported. *Third*, the government itself would buy thousands of units for its own use.

Next came the two positioning decisions. Between deciding on developing its own standard or adopting one from outside, AT&T decided to adopt an outside standard developed by the NSA. The second positioning decision was between keeping it open or proprietary. The NSA was clear about the secretive nature of its algorithm and kept it strictly proprietary. Only AT&T's TSD-3600 contained this advanced encryption albeit with a government backdoor.

Indeed, in February 1994, the federal government officially adopted the technology behind the Clipper Chip as a Federal Information Processing Standard (FIPS) – FIPS 185 - and it formally came to be known as the Escrowed Encryption Standard (EES). According to Froomkin (1996),

FIPS are aimed at efficient procurement and usage of computer and information technologies by the federal government. "FIPS 185 was unusual in that rather than describing the essential, classified parts of the SKIPJACK encryption system or the LEAF creation method, FIPS 185 stated that conforming devices would be certified by the NSA" (Froomkin, 1996).

The second strategic objective of AT&T was **to maximize profits from the established standard.** In the context of networks, a standard becomes more valuable the more people adopt it (Grewal, 2008; Shapiro & Varian, 1999; Grindley, 1995). As is the case in all communication technologies, the AT&T TSD-3600 exhibited *network externalities* or *network effects* as its value depended on wide adoption. Hence it is essential to build a large installed base – a large number of users – quickly. As the installed base grows, more and more users find adoption worthwhile. This pattern of adoption of a standard results from *positive feedback,* a phenomenon that makes large networks grow larger.

The encryption device's success depended on its ability to fuel widespread adoption by the market. A TSD-3600 in possession of a user would have value only if the people they wanted to communicate with also possessed the same AT&T device. "There were concerns that the government's explicit intent to use its market power would shape the business environment by making the technology mandatory. Any company that wished to do business with the government would be forced to adhere to the Clipper standard" (Kehl et al., 2015). The adoption of the Clipper standard by the public was kept voluntary. However, the government planned to use its market power to manipulate the adoption of the Clipper enabled encryption devices. Michael Froomkin (1996) described the method by which the government planned to achieve this.

> "In the absence of any formal authority to prevent the adoption of unescrowed cryptography, Clipper's proponents hit upon the idea of using the government's power as a major consumer of cryptographic products to rig the market. If the government could not prevent the public from using nonconforming products, perhaps it could set the standard by purchasing and deploying large numbers of escrowed products. People who wanted to interoperate with the government's machines would naturally buy the same equipment. The existence of a large functioning user base would create further incentives for others to buy the same equipment."

"The Clipper program attempted to use standardization and federal buying power to influence civilian use of cryptography" (Whitfield & Landau, 2007). AT&T, therefore, relied on government's ability to influence the market and wield network power to help TSD-3600 gain a sufficiently large installed base of users to tip the market.

The third strategic objective for AT&T was to **compete within an established standard effectively in the market.** According to Varian & Shapiro (1999), standards change competition for a market to within a market. Once AT&T's adopted encryption standard was established as the winner, it would need to effectively control the standard in order to retain its power over the field and dictate its meaning and maximize gains from it. AT&T's commercial encryption device, the TSD-3600 went about in its pursuit to ensure that the encryption standard adopted by it effectively dominated the field. This was done in a number of ways primarily through the help of the NSA and the government.

First, to ensure that businesses and individuals adopt the product and thereby lend it greater network credibility, the government opted for "bureaucratic innovation" (Froomkin, 1996). The federal government formally adopted the Clipper Chip as a Federal Information Processing Standard (FIPS) known as Escrowed Encryption Standard. This was combined with a

deal the government had struck with AT&T to be a big purchaser of the product. This meant that the government would use TSD-3600E enabled phones and anyone who wished to do business would also have to acquire the same phone. The devices were priced at $1000 each (Blaze, 2011).

Second, the chips were costly and could only be acquired from a single supplier. The secretive, proprietary and classified nature of the Clipper Chip and the Skipjack algorithm allowed the NSA to retain a firm grip over its standard by denying interoperability. The FIPS, instead of promoting interoperability emerged as a government tool to exercise control over those products (Diffie and Landau, 2007). The EES also stated that the government would decide on which companies would be allowed to include the encryption product.

Third, by having strong encryption placed under the category of munitions and through severe export restrictions, the government hoped to gradually stifle the development of strong commercial encryption by other companies and compel them to conform to the government's standard. We will examine this aspect in greater detail in the next section.

Matt Blaze (2011) posited that communications cryptography, by the 1990s was a "zero-marginal-cost technology", but by deploying encryption in hardware rather than in software the inherent cheap nature of the technology was made artificially expensive. This led to an untenable market situation even if the trust issues and technical problems could have been resolved.

4.4 Software Key Escrow and Export Restrictions: A Post-Clipper Standards War

Despite the government's clout and its backing, it was clear by the fall of 1995 that the Escrowed Encryption Standard and the Clipper Chip wouldn't take off. The essential step of creating a large installed base of users, which is vital for a standard with network externalities,

failed. Total sales of all TSD 3600s stood at about 17,000 of which 9000 Clipper models were bought by the FBI while the rest were shipped to Latin America and the Middle East (Whitfield & Landau, 2007). AT&T was the first and the only company to adopt it commercially in the hope that it would emerge as the market standard.

Amidst a vociferous chorus of united privacy activists, technologists, academics, hackers and industry leaders against an encryption standard with a mandated backdoor for government access, a young researcher at AT&T's Bell Laboratories named Matt Blaze exposed a vital flaw in the Skipjack algorithm. His paper, published in April 1994, dealt a "death blow" to the Clipper Chip by exposing a fatal flaw in its architecture. Blaze demonstrated that a brute force attack could circumvent the law enforcement surveillance mechanism (Kehl et al., 2015). A report published by the Open Technology Institute asserts that "the fact that the government could be shut out of its own surveillance protocol suggested that it was not qualified to be dictating technical mandates like the Clipper Chip at all" (2015).

Thus, with the eventual demise of the Clipper Chip and the Escrowed Encryption Standard, the challengers in the encryption field had dealt a severe blow to the credibility of the incumbent's privilege to set the rules and define the meaning of the space. The market had summarily rejected the government's standard within the sub-field of commercial encryption. Although not an actor in the sub-field that was populated by technology companies, the government used its influence in the larger encryption field to influence the sub-field. The market, however, refused a standard that wasn't suited to its demands.

Two important aspects of the government-backed standard stand out. *First*, despite offering a stronger 80-bit protection for telephone communication, the existence of a government backdoor emerged as a threat to privacy and was viewed as unacceptable. *Second*, the discovery

of a fatal vulnerability rendered the standard inadmissible in an organizational field that was run by market driven innovation. Despite the demise of the Clipper Chip, the government did not abandon its attempt to control cryptography after 1995 (Kehl et at., 2015). The strategy had now shifted towards "software key escrow" instead of hardware escrowed encryption in the TSD-3600s. It also came to be known as "commercial key escrow" or "key recovery" schemes.

4.5 Software Key Escrow / Key Recovery: A Second Attempt at Field Dominance

Despite the demise of the Clipper Chip in hardware, the government planned to pursue its standard of escrowed encryption in the commercial sub-field. This move characterized a second phase in the government's push to establish its standard. Software key escrow differed from the Clipper Chip in a number of respects. Rather than embedding a physical chip in hardware, the proposal was to convince companies to implement a key escrow system themselves. The keys would be deposited with certified private escrow agents rather than directly with the government. NIST issued a set of ten principles or "The Ten Commandments" (Diffie & Landau, 2007) to the industry regarding software escrow, which sought to set the standard requirements for implementing encryption in commercial products. These "commandments" dangled a significant carrot: they would relax encryption export controls in exchange for agreeing to the standards demands by the government. The requirements sought to i) limit the key length to 64-bits, ii) Such systems must allow recovery of the key from traffic in either direction, iii) They must not interoperate with unescrowed versions of the same systems. Further iterations of the proposal in the fall of 1996 offered a new incentive: For two years, beginning on January 1, 1997, "the government would allow export of unescrowed systems with 56-bit keys in return for promises from the exporters that they would implement key-recovery systems in their products"(Diffie & Landau, 2007). The government was attempting to have its standard established in the

commercial realm by cajoling the challengers into accepting it.

The standards proposals were ultimately no more palatable than the original Clipper Chip because of the government's insistence that a backdoor into any domestic or exported encryption product must exist. However, from a market perspective, this would result in a weak encryption standard and consequently a weak product that would find it hard to compete internationally and domestically. This would hurt the actors who would invest in encryption technology with the intent of making profits.

4.6 Export Restrictions

Historically, cryptographic tools had been the sole domain of military and intelligence agencies. Prior to 1996, all products using encryption were controlled under the International Traffic in Arms Regulation (ITAR) and listed on the US Munitions List (USML). Any encryption over 40-bits was considered "strong encryption". Products that fell under the ITAR needed a separate license application and review which involves a referral to the Defense Department and the National Security Agency. However, as the 1990s dawned and encryption rapidly gained commercial market value, keeping it under USML became increasingly difficult to justify. Writing in 1996, Michael Froomkin remarked "for the past two decades or more, a major goal of U.S. cryptography policy-to the extent that the U.S. has had ones-has been to prevent strong mass-market cryptography from becoming widely available abroad, with export controls being the primary tool used to achieve this end."

From a standards perspective, the export restriction of tools with keys longer than 40-bits would also serve to ensure that the government issued standard would benefit domestically by preventing companies from exporting strong cryptographic products overseas. At a time when

the DES encryption itself was 56-bits, a crypto product with a 40-bit key was one that the government could easily decrypt. Some in the technology industry even referred to the 40-bit limit as "espionage enabled encryption*"* (Diffie & Landau, 2007). Journalist Steven Levy called it "crypto-lite".

This proposal left the companies with essentially two choices. They could, like Lotus, offer two different versions of the same product--a strong 64-bit encryption for domestic users within the US and a second 40-bit encryption version overseas. Or, like Microsoft, they could avoid the hassle of manufacturing and shipping two separate versions and produce a single version with lower encryption standard that was much weaker. The government could ensure in two ways that a strong export restriction would lead to weaker crypto products domestically. The first method was through its licensing regime. By requiring companies to gain approval before exporting crypto products, the US government could effectively control the commercial proliferation of the technology. "It could look favorably upon certain types of products and deny licenses to ones it deemed too strong" (Kehl et al., 2015). By doing so it could indirectly coerce companies to adopt an encryption algorithm in their products that was more likely to get a license.

The second method was cost imposition. As discussed above, companies were left with two choices – the Lotus option or the Microsoft one. Not all companies had the means to manufacture, market and ship two versions of the same product. Therefore, they would be compelled to produce only the weaker 40-bit version both internationally and domestically. In this context, the government's carrot-dangling of allowing up to 64-bit encryption to be exported provided they adhered to the software escrow demands. A report from the U.S. Department of Commerce and the NSA did acknowledge that some American businesses "believe that not being

able to participate at the early stage of market development will be a tremendous obstacle to their future international competitiveness" (Kehl et al., 2015). From a standards perspective, a first-mover advantage is often vital to the establishment of a winning standard. The conventional wisdom in the highly competitive software industry holds that any delay may be fatal to a new product's marketability. Routine export applications are approved quickly, but an ambitious application can meander through the administrative appeals process.

Faced with the challenge of adherence to a weaker standard in the highly competitive arena, by the mid-1990s companies began to voice their opposition strongly. A study by the Economic Strategy Institute in 1998 projected estimated losses between $35 and $95 billion due to the standard imposed by the government and its export restrictions. In June 1999, another report by the Cyberspace Policy Institute at George Washington University noted that there were over 500 foreign companies engaged in manufacturing crypto products in nearly 70 countries (Kehl et al., 2015).

4.7 A Phase Transition: Towards a New Equilibrium in the Field

The defeat of the Clipper Chip by 1996 signaled a sure sign of major eruptions within the field as the standard set by the incumbent NSA failed to take off in the open market. This emboldened the challengers who had been campaigning for escrow free encryption without government access. By 1997, the upheaval within the field calling for looser export restrictions had gained steam. In November 1996, A White House Executive Order (13026) officially acknowledged encryption as a commercial tool by handing it over to the Department of Commerce's Export Administration Regulations (EAR) (Kehl et al., 2015). The move allowed the export of encryption software up to 64-bits, but still required a license to do so. The shift marked a first step towards broad liberalization of encryption export.

Meanwhile, the National Research Council (NRC) that was tasked by the Clinton Administration to conduct an in-depth study into encryption came out with its 500-page report in June 1996. A classified report that was declassified by the Central Intelligence Agency (CIA) in 2014 states that the NRC report was highly critical of the Clinton administration (Schwartzbeck, 2014). The report did not take lightly to the manipulation of encryption through arms control laws and concluded that "widespread commercial and private use cryptography is inevitable in the long run… and its benefits outweigh its disadvantages" (CRISIS, 1996). Moreover, Congress saw two bills introduced in support of strong encryption technology.

In September 1998, Vice-President Al Gore introduced more concessions as he announced the opening up of export of strong encryption for commercial purposes. Companies could now export both hardware and software crypto products containing 56-bit keys without a license. Additionally, they were not required to submit key-recovery plans either. On September 16, 1999, the White House announced that it intended to "significantly update and simplify export controls on encryption". Finally, at the dawn of a new millennium in January 2000, the Commerce Department released the revised regulations, which amended the Export Administration Regulations. Strong commercial encryption tools could freely be exported globally.

As the Crypto Wars drew to a close the broad policy consensus in the US was to allow American citizens to choose strong encryption and companies to create strong encryption for sale within and outside the United States. The failure of the NSA to hold on to its monopoly over crypto tools and its eventual defeat(s) in the standards war can be characterized as a "phase transition" – "a gradual build up over time followed by a sudden and total restructuring of the field" (Perez, 2009; Padget & Powell, 2012 as cited in Garcia, 2016). Garcia (2016) cites "four

interdependent factors" that contribute to the phase transition, all of which do apply to our case at hand. *First,* technological developments in encryption technology meant that strong tools were now available commercially for individuals and businesses to make use of. The tools were stronger and more secure in that they could prevent government eavesdropping or access. *Second,* economic developments ensured a steady growth in public demand for encryption technology. An explosion in the adoption of PCs and mobile phones coupled with the rise of the internet warranted the use of encryption to protect confidential data and communications. This justified the developments of commercial products by companies. *Third,* changes in regulation opened a new vista of opportunities where crypto tools were no longer considered as munitions and could be exported freely without government approval or licensing. This led to market driven innovation and internationally competitive US products. *Fourth,* opening of the international markets competition meant that companies could now market their products beyond American shores and compete globally. This not only created greater incentives for the encryption field to innovate but also invest in setting stronger standards that could be applied internationally.

Thus, a new equilibrium was achieved after years of upheaval with the arrival of new incumbents. The US technology companies, who had emerged as the challengers in the early nineties, had now redefined the meaning of the commercial encryption field and seated themselves as the incumbents. Indeed, the ability to create, use and disseminate strong encryption without government mandated backdoors or restrictions on export meant that the rules of the field had transformed into those fought for by the technology companies, public researchers, privacy advocates and corporate investors. A new field with a new equilibrium had emerged at the dawn of the new millennium.

Chapter 5: Standards Contest in the Encryption Field – Crypto Wars 2.0

5.1 Introduction

This chapter conceptualizes the stalemate between the technology industry and law enforcement agencies in Crypto Wars 2.0 from an organizational field perspective with actors vying for dominance of the field. Similar to the analysis in the previous chapter, which explored the encryption field of the 1990s as a war of standards, this chapter, too, examines the commercial encryption field in mobile phones as a standards contest and looks at the field between 2010 and 2016.

In particular, this chapter looks at how "exogenous shocks" from outside the field can lead to turbulence within the field, disturb the stability and 'agreed upon meanings," which calls for action by the incumbents and challengers to mitigate the shocks and period of contention. In the last chapter we saw the emergence of a new organizational field where the initial challengers emerged as the incumbents and thereby redefined the rules as well as the structure of the contested arena. The Crypto War as a standards war in the commercial encryption field came to an end in 2000 with a victory for the technology companies. The new standards established within the field favored the production, use and sale of strong encryption without mandated backdoors for intelligence, law enforcement wings of the government. The new standards paved the way for US citizens to have access to strong crypto tools and thereby enjoy a greater standard of privacy. The imposition of costs and the accruing financial losses were unacceptable to a field that operated within a competitive domestic and internal market environment.

As defined in the previous chapter, organizational fields are "highly contested arenas" (Garcia, 2013) characterized by "ongoing internal tension between incumbents and challengers" (Fligstein & McAdam). We interpret these "tensions" and strategic jockeying for power within the field and its broad environment as a standard contest, and employ a standards framework to analyze the progress of Crypto Wars 2.0.

This chapter first defines the organizational field, the actors and the technology. It then breaks down the second Crypto War into three major chronological segments – Going Dark, The Snowden Shock and the FBI vs Apple court case. The phrase "Going Dark", first framed in 2011 by the FBI, recounts the renewed call by law enforcement agencies to alter the prevalent standards in the commercial encryption field. The paper considers this as the starting point of "Crypto Wars 2.0," which eventually erupted in a public showdown between the FBI (Department of Justice) and Apple Inc. in 2016. The second phase looks at former NSA contractor Edward Snowden's leaks to the media that revealed pervasive snooping by the NSA. The significance of this event lies in the subsequent strengthening of encryption by technology companies in the wake of the revelations. We will be exploring this issue as an event in a proximate field, which led to turbulence within the encryption field. The third phase of this section is the FBI vs Apple debate which studies the one-and-a-half month long court battle over the encryption of an Apple iPhone 5C.

Within these three sub-sections we structure the "revisionist" account of Crypto War 2.0 around the following five key concepts of organizational field theory (Fligstein & McAdam, 2012):

- Organizational Field: Before
- Exogenous Shocks

- Crisis and Contention
- Stability and order
- Effect on other organizational fields and the broad environment.

5.2 Defining the Field

We define our organizational field of interest in this chapter as "*The US Smartphone Operating System Encryption Field*" or "*US Smartphone OS Encryption Field*". Henceforth, this paper will refer to Operating Systems as "OS" as it is more commonly referred to. An important feature of this field that distinguishes it from our study of the first Crypto War is that this is an already established and relatively stable field with well-defined actors, boundaries and understanding of rules, positions and structures. Additionally, its broader field environment including proximate and dependent fields are also well defined and established.

In 2011-- the starting point of our study of Crypto Wars 2.0--the field had clearly defined incumbents and challengers as well as internal governance units. While Apple Inc. and Android (owned by Google) are defined as the incumbent actors based on the lion's share of resources, installed base and revenues they command, smaller players like Microsoft's Windows OS and BlackBerry OS are seen as the challengers because of the meager share of the field's customer base and profits they have access to. By virtue of collectively dominating the US field, Apple's iOS and Google's Android OS do wield disproportionate influence within the field as incumbents, and have adapted it to their interests. In addition, the rules of the field tend to favor their positions while the shared meanings are designed to legitimize and support their privileged positions (Fligstein & McAdam, 2012).

Encryption software in smartphones are a product of the OS. Hence Apple's iOS, Google's Android OS also compete on the strength of the privacy protections and security they provide through the encryption in their software. As mobile phones grow "smarter" they increasingly offer a greater variety of services and products, which results in a much larger amount of personal information and data stored within them. Smartphones today offer between 8 Gigabytes (GB) and 128 GB of data storage in a single unit and, in reality, are mini computers with advanced operating systems that also allow users to make calls and send texts (Grimmelmann, 2016). Given the amount and value of data stored within a smartphone today, in-built encryption has indeed emerged as a vital feature of OS.

In this context, there are two kinds of software encryption – for data at rest and data in motion. Data at rest encryption refers to data stored in smartphones, tablets and PCs and laptops. This form of encryption that secures this stored data is known as "full disk encryption". The other form, data in motion, refers to data contained in communication services like messaging apps, e-mails and texts between two or more people. The encryption that secures this data in transit is known as end-to-end encryption. The type of encryption that concerns the FBI vs Apple battle in 2016 is the full-disk encryption of data at rest.

Actors within the "*US Smartphone OS Encryption Field*" are also affected by the US government and its different branches – the legislative, executive and judiciary – all of which form separate fields of their own. Fligstein and McAdam (2012) describe the state fields as "dense system of interdependent fields" which possess "considerable and generally unrivalled potential to affect the stability of most strategic action fields". They also posit that "stability of any given field is largely a function of its relations to other fields" (2012). While fields can spiral into conflict on their own, it is more common for "episodes of contention" and turbulence within

a field to arise out of "exogenous shocks" or change pressures emanating from other proximate state and/or non-state fields. In this context, the actions of the each of the three branches of government have the potential to upset the stability and order of our field of interest. Since the FBI, which is housed within the Department of Justice, which in turn is a federal executive department of the U.S Government, has to work in co-operation with technology companies for its investigations, it has a vested interest in the operations of *US Smartphone OS Encryption Field*. Although it has no commercial stake in the field, it does have a professional interest because strong encryption impedes its ability to gain access to communications, data and information that it requires to carry its investigations. Thus, we can say that developments within the *US Smartphone OS Encryption Field* can alter the nature of FBI investigations. Law enforcement agencies such as the FBI, then, are not only affected in terms of its access to information but also in terms of cost as it must keep itself technically up to speed with the innovations in the encryption fields.

An important hypothesis we will be testing is the ability of the FBI as an organizational field to change the encryption field.

Hypothesis: The Department of Justice can cause an episode of contention within "US Smartphone OS Encryption Field" but cannot alter its nature.

5.3 "Going Dark": Rumblings in a Stable Organization Field (2011)

This section looks at the encryption field at the beginning of Crypto Wars 2.0 and discusses the factors that led to an initial jolt to the "US Smartphone OS Encryption Field". We begin by charting the developments between the end of Crypto Wars 1.0 and the beginning of Crypto Wars 2.0. Having laid the ground for contextualizing the technological and political environment

leading to the first signs of a new crypto war we analyze the "going dark" phase and interpret it from an organizational field perspective.

5.3.1 The Inter-Crypto War Years: 2000 – 2011

The first crypto war ended with the challengers assuming the role of the incumbents. The technology companies that fought a decade long battle for higher encryption standards thereby mounting a relentless challenge to the standards enacted by the NSA and then the US Government in communication technology won the battle in 2000. The standards war ended in favor of robust encryption. The standards established by the new incumbents not only changed the rules of the game but also engendered a new meaning system. It became increasingly clear to the field as well as the US Government that society was in favor of greater privacy protections and the rise of new mobile and computer technology had generated a great demand for secure and strong encryption tools.

The new state of equilibrium and order in the field encouraged the production, use and sale of strong commercial cryptographic tools. It also warranted the continued innovation of these products based on market competition. Moreover, cryptographic tools for civilian use were no longer listed as munitions and were no longer subject to export restrictions and stringent licensing regimes monitored by the government. The dawn of a new millennium ushered a new dawn in the encryption field as well. Technology companies, scientific researchers and independent studies all concluded that the benefits of strong encryption outweighed the disadvantages.

Primarily, two major trends have redefined the landscape of the battle since the first crypto war ended in 2000. According to Jonathan Zittrain (2016), the first arises from the

terrorist attacks of 9/11. The attacks on the World Trade Center in New York "reshaped the priorities of the U.S intelligence community, as extraordinary resources have been allocated to prevent and counter terrorism". The second trend is the "mainstreaming of the Internet and surrounding technologies built around and upon it, which has led to an unprecedented amount of data that can be analyzed by the intelligence services" (2016). It is in this context that the terms "national security" assumed new meaning and significance in the debate. On the other hand, the internet boom in computers and subsequently in smartphones fueled the rise of e-commerce. This period saw the emergence of encryption protocol standards like the Secure Socket Layer (SSL) and its successor, Transport Security Layer (TLS), as well as the adoption of HTTPS. This new ecosystem of secure digital communications has enabled the rapid rise of social networks, electronic banking, e-medical record systems and financial transactions.

5.3.2 "Going Dark": 2011

The smartphone market in the US and around the globe had grown rapidly as well. According to reports, the US had 92.8million smartphone users in 2011 and that same year the number of users in the world stood at 700million. This rise also engendered a demand for stronger privacy protections of information, data and communications, which led to increasingly strong encryption in devices and communications to meet the needs and demands of the market.

It was in this context that Valerie Caproni, the FBI's then-General Counsel, testified before the House Judiciary Committee on February 17, 2011 and used the phrase "going dark". The phrase was meant to describe the government's impediments towards access to communications in the face of growing encryption.

Describing "going dark" as a "problem", Caproni testified,

> "As the gap between authority and capability widens, the government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage—evidence that a court has authorized the government to collect. This gap poses a growing threat to public safety (2011)."

Even though in her testimony Caproni specifically mentioned that the problem lay in access to stored data but in the "interception of electronic communications and related data in real or near-real time", later iterations of the phrase by the FBI would also include data at rest and encryption in general. This FBI has led the government's participation in the current debate just as the NSA had done two decades ago.

From a field theory perspective, this represented a first attack on the *US Smartphone OS Encryption Field* from a proximate state field. Given the dependent nature of the fields, an appeal to modify the operating standards was expected to create ripples within the broad encryption field and its sub-fields such as the *US Smartphone OS Encryption Field*. However, the technology companies that operate as actors within the encryption fields did have a number of inherent concerns with any architecture that guarantees access to the government. *First,* such access would compromise the security of digital communications that foreground secure communications over the internet. *Second,* it would lead to a violation of privacy of those who communicate over the internet. *Third,* it would hurt the viability of US companies worldwide. Technology companies worried that it would erode the trust among users of encryption enabled digital software and drive competition to other foreign companies. The demands by law enforcement weren't aimed at a particular company at this point but could potentially impact the stability of the entire field. The

incumbent actors as well as the challengers would have to decide on a strategy to combat it. While the incumbents would need to rally the field around a common cause, challengers would need to decide whether to stand by incumbents or use this as an opportunity to better their positions. Most incumbents, however, are well positioned to weather such storms.

5.4 Snowden and Exogenous Shocks in the Field (2013 – 2014)

Two years after the FBI used the phrase "going dark", a new series of events sparked a new phase in Crypto War 2.0. The publication of then NSA contractor Edward Snowden's revelations in June, 2013, about US intelligence's surveillance of US citizens once again catapulted the debate of privacy versus national security on the front pages and headlines around the US and the world. This section looks at events of 2013 and 2014 in the context of Crypto Wars 2.0 and explores its implications for the US Smartphone OS Encryption Field.

5.4.1 The Snowden Leaks

On June 6, 2013, British newspaper, *The Guardian*, published a report revealing that "The National Security Agency is currently collecting the telephone records of millions of US customers of Verizon, one of America's largest telecoms providers, under a top secret court order issued in April". The order, issued by the Foreign Intelligence Surveillance Court (FISC), also known as the FISA court, required Verizon, one of the largest telephone and internet service provider (ISP) in the US, to provide NSA informational on all telephone calls in its systems on an "ongoing and daily basis", both within the US and other countries. It was gradually revealed that other telephone companies were ordered to comply in a similar manner.

Twenty-four hours later, on June 7, a larger revelation awaited as both *The Guardian* and *The Washington Post* ran a story stating that the NSA had direct access to the systems of Apple,

Google, Facebook, Microsoft among others through a special program known as Prism, a surveillance program, that was launched in 2007. The program was believed to help NSA "receive" emails, video clips, photos, voice and video calls. It was later established that the NSA might not have had “direct access” but did nonetheless receive information through the digital equivalent of locked mailboxes. While the revelations continued for nearly a year and into the summer of 2014, among the major news items were reports of the NSA and its British counterpart, the Government Communications Headquarters (GCHQ), had spied on European Union (EU) nationals including the Chancellor of Germany, Angela Merkel. China, Hong Kong, Brazil, among a host of other major economies had their networks surveilled, according to reports published. While the entire breadth of Edward Snowden’s leaks and the revelations made in the aftermath of his handing over of 1.5 million documents lies beyond the scope of this paper, the event did serve as a significant landmark in what would come to be regarded as the second installment of the Crypto Wars. “Beginning in 2000, as encryption tools were gradually blanketing the Web, the NSA invested billions of dollars in a clandestine campaign to preserve its ability to eavesdrop. Having lost a public battle in the 1990s to insert its own “back door” in all encryption, it set out to accomplish the same goal by stealth”, a New York Times report read (September 5, 2013).

5.4.2 Turbulence in the Encryption Field

The Snowden leaks cast a shadow of doubt over the adequacy of encryption standards set by the incumbent actors in the field. It also raised concerns about consumer trust in the ability of smartphones to protect their information and communications through current encryption standards. While the revelations directly impacted the status quo of the law enforcement and intelligence fields, its ripples were felt in the encryption fields as they challenged the credibility

of encryption tools installed in phones and computers. Fligstein and MacAdam (2012) describe this as ripples emanating in a pond that disturb proximate fields as well. In this context, Apple responded to allegations of providing exceptional access into their systems with outright denial and swiftly moved to allay fears of its installed base. A letter reiterating Apple's "commitment to consumer privacy" explicitly states that the company does not "provide any government agency with direct access to our servers, and any government agency requesting customer content must get a court order" (Jun 6, 2013).

Over a year later, on September 18, 2014, Apple launched the latest version of its operating system, iOS 8. This version contained significant alterations to the privacy settings for the iPhone, iPad and the iPod and was guided by a radically new privacy policy. Apple's new policy not only set new standards for itself but also proposed an overhaul of the prevalent standards within the "*US Smartphone OS Encryption Field*". *First,* Apple locked itself out from the data stored in an iPhone. Once a user sets a passcode, the OS automatically encrypts the data within the phone in a way that ensures even "Apple cannot bypass your passcode and therefore cannot access this data" (2014). This was an unprecedented act and one that would have serious implications for the intelligence and law enforcement communities. *Second,* Apple extended its OS encryption to nearly all the data contained in the iPhone through its full-disk encryption, including texts and photographs, which were previously not encrypted. Personal data such as photos, messages, email, contacts, call history, iTunes content, notes, and reminders were placed under the protection of the user's passcode. Meanwhile, communication applications in the iPhone such as iMessage and FaceTime were protected with end-to-end encryption. *Third,* iOS 8 introduced a time delay between passcode attempts and incorrect passcode will multiple the length of delay between attempts. This is aimed at thwarting brute-force attacks to break into

the phone by trying every combination of 4-digit or 6-digit passcodes. According to the company's security literature, this means that it would take a brute-force attacker five-and-a-half years to try all combinations of a 6-digit alpha-numeric passcode with lower-case letters and numbers.

Google, which runs the Android OS, followed suit and on October 15, officially launched its latest OS, Android 5.0 "Lollipop" which implemented the same encryption practices announced by Apple for its iOS 8 version a month earlier. Regarding security, Google announced that Lollipop had the "biggest update for Android till date" (October 28, 2015). It promised default encryption for the first time and also offered to render itself incapable of breaking into a user's phone. A spokesperson for Google was quoted stating, "For over three years Android has offered encryption, and keys are not stored off of the device, so they cannot be shared with law enforcement," (*Washington Post*, September 18).

Therefore, with these new encryption standards in place, both incumbent actors, Apple and Google, appeared to be on the same page regarding the rules they wanted to establish in the field. Irked by the Snowden-induced ripples emanating from proximate fields, both incumbents acted to mitigate the fears of instability within the field by redefining the standards to which the field should adhere. By doing so, the incumbents managed to restore order within the field through the establishment of a higher level of encryption. Another significant standard set by the field collectively was to move towards a greater level of transparency with its installed base. In order to allay fears and restore trust among customers after the Snowden revelations, the incumbents as well as the challengers had appealed to the Department of Justice to be allowed to share more information about the amount of customer data they are compelled to share with the

government. This transparency initiative was intended to compliment the enhanced encryption in order to assure the installed base of their privacy protections.

An important implication lay in Apple's swift move to raise its encryption standards. While both Apple and Google are identified as incumbent actors within the *US Smartphone OS Encryption Field*, in terms of their installed base and market share Google Android OS has a larger slice of the pie (see figure 2). Both, domestically as well as globally Android has more users than iOS. Despite being the smaller incumbent actor Apple announced its standards first. By doing so it gained a first mover advantage and did affect a change in the field's established meaning system. Google, despite being the bigger of the incumbents, followed suit and adopted the same standards announced by its incumbent partner. Sensing an opportunity in the partial instability caused by ripples sent out from the US intelligence field, Apple managed to have its rules stamped as dominant. While this did not result in Apple overtaking Google's installed base, it did provide the Cupertino based company leverage in acting as the lead incumbent.

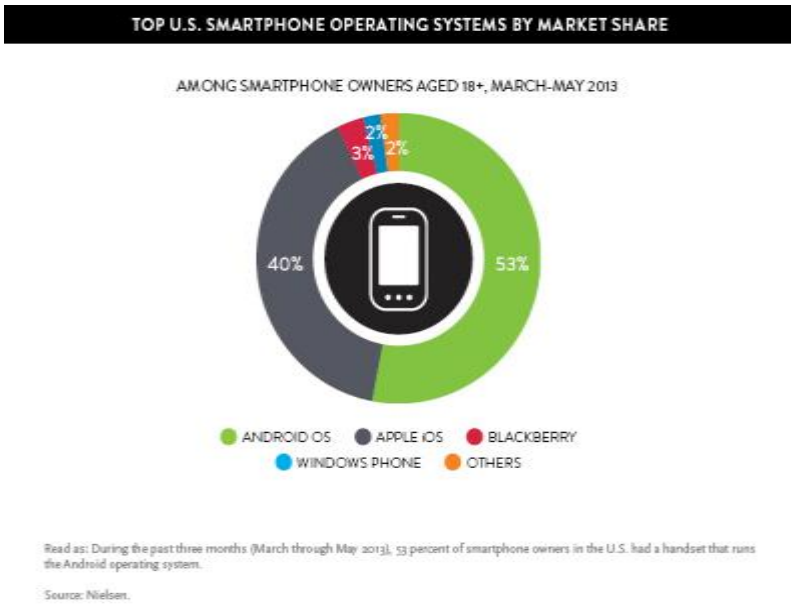

Fig. 2: US Smartphone OS Market Share in 2013. Source: Nielson

5.5 FBI vs Apple (2016): An Episode of Contention

An imposition of a genuine crisis in organizational fields is rare despite frequent tension caused by the broader field environment. Fligstein and McAdam (2012) state that the extent of the threat that is posed by the destabilizing change can be determined by the "highly contingent mobilization process."

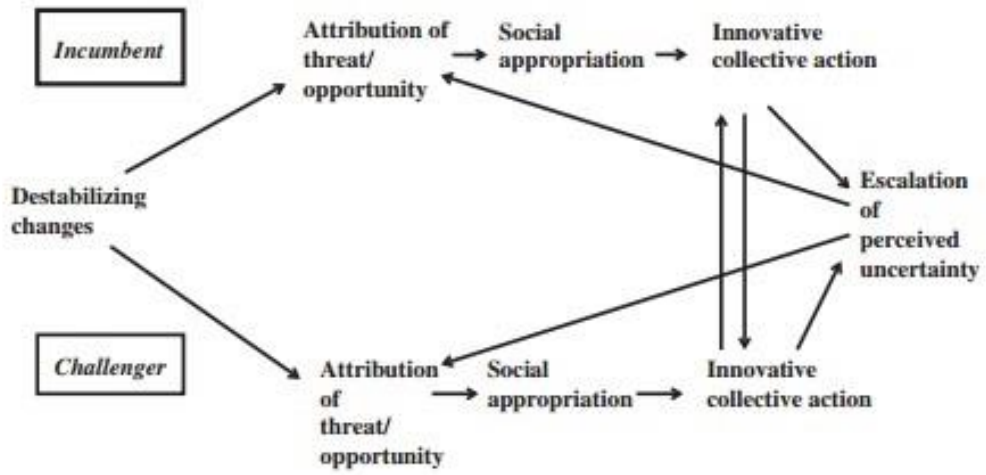

Fig. 3: Fligstein & McAdam's Mobilization Process Framework (2012)

This organizational framework proposed by Fligstein and Mc Adam (2012) provide a useful method to explain the FBI vs Apple legal controversy as a field crisis or "an episode of contention". The authors define an episode of contention as "a period of emergent, sustained contentious interaction between…[field] actors utilizing new and innovative forms of action vis-a-vis one another" (McAdam, 2007: 253).

In the context of Crypto War 2.0 the episode of the FBI vs Apple legal battle serves as an episode of crisis that could potentially undermine the existing dominant rules of the *US Smartphone OS Encryption Field*. Indeed, by asking the judicial branch of the government to intervene in the deadlock over providing exceptional access into Farook's iPhone, the FBI sought to undermine the established standards in the encryption field. The California court's order to Apple would effectively decrease the strength of the encryption standards that had been established since the launch of iOS 8 in 2014. If the FBI could successfully get Apple to create a "backdoor" into the particular iPhone 5C through judicial intervention, it would have the potential to undermine and alter the existing status quo of the field altogether. This presents a unique case of an actor from a different field acting as a challenger. The FBI as an external challenger is observed as trying to bring a change in the adopted standards of the *US Smartphone OS Encryption Field*. A lowering of the standards of encryption within the field would stand to benefit the FBI by giving it easier access into communications and stored data and, perhaps, solve the "going dark" issue.

Before we move into a discussion of the mobilization process in order to describe the episode of contention, it is important to list the factors that spurred this onset of contention. We have namely identified three factors. *First,* the "going dark" debate initiated by the FBI in 2011. *Second,* Apple's launch of iOS 8, which significantly enhanced the encryption standards within the field. Later versions of the iOS (iOS 9) as well upheld these enhancements. *Third,* the San Bernadino shootout on December 2, 2015, which provided the FBI with an opportunity to pressure Apple into modifying its encryption and thereby set a legal precedent.

Fligstein and McAdam (2012) state that the mobilization process consists of three linked mechanisms. The first is the collective *attribution of threat/opportunity*. The question here is,

how are the destabilizing interruptions interpreted by the incumbents and challengers of the *US Smartphone OS Encryption Field*? Unless the shocks are viewed "as a serious threat to, or opportunity for realization of collective interests" (2012), there is little possibility for the development of an "episode of contention" (2012). Indeed, faced with the potentially destabilizing attack by an external challenger, Apple interpreted FBI's court order as a serious threat to the entire encryption field. By doing so it also conceptualized the threat as an opportunity to reassert its own dominance within the encryption field. As an incumbent actor, Apple did manage to rally a collective attribution of opportunity by framing the threat by an external challenger, such as the FBI, as not just a threat to Apple but to the entire encryption field. In doing so, Tim Cook's company successfully managed to mobilize all the actors, incumbents as well as challengers, of the encryption fields to resist this threat to their field.

Two other events must accompany the attribution of threat/opportunity in order to spark an episode of contention (Fligstein & McAdam, 2012). *First*, the effective utilization of available resources by actors who have initiated the perception of threat/opportunity. This is referred to as *social appropriation* (figure 3). From the field perspective, Apple did "appropriate" the social narrative of US privacy rights. By portraying itself as a champion of the privacy rights of American citizens, Apple not only invoked the concept of patriotism but also pushed the larger issue of privacy in the context of this legal battle. In a letter published on February 16, the day the California court ordered Apple to assist the FBI in unlocking the phone, Tim Cook addressed the American people directly. This address was significant because he did so even before he responded officially to the court order. Describing the court order as "fear that this demand would undermine the very freedoms and liberty our government is meant to protect", Cook wrote,

> "If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge." (Feb 16, 2016)

A relevant concept of this stage of the *mobilization process* is "framing" through which an "incumbent actor may seek to enlist the support of its allies within and outside the field around a particular conception of the field" (Fligstein & McAdam, 2012). The successful mobilization of actors from within and other proximate fields is evident in the number of amicus briefs it received from Silicon Valley, privacy advocacy groups and industry associations. While actors within the encryption field like Google and Microsoft filed briefs in support of Apple's position, proximate field actors like Facebook, Twitter, Snapchat, Yahoo followed suit. Industry associations like BSA – The Software Alliance, The Consumer Technology Association and the Information Technology Industry Council registered their support for Apple as well through their amicus briefs. Also, policy making bodies, think tanks and advocacy groups like Center for Democracy and technology, Electronic Frontier Foundation, Electronic Privacy Information Center (EPIC) and Human Rights Watch, among others joined in as well. This show of support demonstrates the mobilization around a common conception of the field.

Apple, therefore, can be said to have framed the legal battle as an assault on privacy rights. By framing encryption as a pillar of privacy, Apple effectively framed itself as a protector of privacy by providing a high standard of encryption in its OS platforms. In a sub-heading titled

"The Need for Encryption", Tim Cook's letter expressed that "for many years, we have used encryption to protect our customers' personal data because we believe it's the only way to keep their information safe. We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business" (2016).

Apart from social appropriation, the second factor in the mobilization process that drives the onset of an episode of contention is *innovative action* (Fligstein & McAdam, 2012). It is described as "the heightened interaction involving the use of innovative and previously prohibited forms of collective action as a hallmark of an episode of contention" (2012). In this context, we can interpret Apple's subsequent actions in the FBI vs Apple episode as an example of "innovative action". As revealed by Apple and other technology companies, they routinely receive hundreds of request from law enforcement agencies to assist them by providing access to data of their customers. Some of those requests do end up in litigation where courts are asked to intervene. However, by publishing a public letter to its customers immediately after the court order on February 16, Apple CEO, Tim Cook, transformed a routine legal process into a national public debate on privacy versus national security. Indeed, by pushing encryption into the front pages of newspapers through the national debate, Apple successfully managed to engage myriad actors from within and outside its field into collectively joining in the protest to the challenge mounted by the FBI on the *US Smartphone OS Encryption Field*. Apple had published the letter publicly even before it formally replied to the court order and filed its legal brief in the case. The Cupertino based company explicitly stated its opposition to FBI and the court order among the public much before it did so in its formal legal reply.

By explicitly calling for a "public discussion" so that "customers and people around the country understand what is at stake"(Cook, 2016) , the FBI vs Apple legal drama, therefore,

transformed into a nationally debated public issue. It engaged the national and international media, policy makers, civil liberties advocates, technology community and most importantly Apple's own installed base of iPhone users. Another important aspect of this was the unification of the incumbents and challengers around the mobilization of this narrative. Google, the other incumbent and challengers like Microsoft, BlackBerry joined in their support of Apple's position on encryption and privacy. The successful enlisting of all actors into collectively joining the case was achieved by effectively framing FBI's challenge as a threat to the entire field. Apple's decision to engage in *innovative action*, therefore, turned an esoteric legal battle into an internationally publicized and nationally engaged public drama. The FBI vs Apple debate was effectively transformed into a privacy vs national security debate. Apple, of course, framed itself as fighting on the side of privacy in this nationally important debate.

Fligstein and McAdam (2012) assert, that besides innovative action, contentious episodes also contain a shared sense of uncertainty. This uncertainty pertains to the rules and the power relations governing the field. Indeed, as discussed earlier, FBI's decision to knock on the court's door to intervene in getting Apple to provide exceptional access into their encryption design posed a threat to the legitimacy and established rules of the field as a whole. If an incumbent actor such as Apple could be forced to lower the standards it had set upon the field, an external challenger like the FBI could effectively alter the nature of the field and dictate terms to all actors. This could undermine the potential of challengers within the field to assert their alternative vision for the field as well. Therefore, we can interpret the court order as triggering uncertainty within the field. "An episode of contention is expected to last as long as this shared sense of uncertainty regarding the structure of dominant order of the field persists" (2012). Indeed, this pervading sense of uncertainty reinforces the perception of threat/opportunity,

which, in turn, recreates the sense of uncertainty. This feeding mechanism, once enforced in the mobilization process, can change the "consciousness of field actors by questioning the rules of the game, the cost and benefits of those rules and power relations among actors in the field" (McAdam & Scott, 2005, p.18-19). The incumbents would see fit to appeal to the status quo in an effort to stabilize the situation.

An important factor in this stage of the mobilization process is the challenger's ability to reinforce that sense of uncertainty and prevent the reassertion by incumbents of the old consensus. To that end, the ability of the challenger to reinforce uncertainty depends on some level of *environmental vulnerability* (2012). The FBI, as an external challenger to the encryption field, can be seen to reinforce the atmosphere of uncertainty by filing legal briefs in quick succession. After the first court order on February 16, the Department of Justice moved court once again on February 19 by filing a second legal brief and then sparring with Apple before Congress at a House Judiciary Committee hearing. The environmental vulnerability was triggered by the San Bernadino incident. While Apple had framed the debate as a fight for privacy rights, the FBI was trying to frame the same debate as a crusade for national security. By referring to the attacks of San Bernadino, in which 14 people died and 22 were injured, as an act of terrorism with alleged ties to ISIS, the law enforcement agency tried to sustain the vulnerability of the encryption field's environment.

5.5.1 Towards a Settlement

On March 28, 2016, in a surprise move, the Department of Justice called off its scheduled hearing with the Cupertino-based company and withdrew its case from the California court. The Justice Department declared that FBI had managed to unlock the iPhone 5C with the help of an external third-party. It no longer needed to compel Apple's assistance in their efforts to get into

the phone. A two-paragraph filing by the DoJ read it had "now successfully accessed the data stored on Farook's iPhone and therefore no longer requires the assistance from Apple."

The episode of contention, thus, came to end with the challenger voluntarily withdrawing its attacks upon the *US Smartphone OS Encryption Field*. This ended the sense of uncertainty that fed the perception of threat. As the potentially destabilizing change subsided, the field once again returned to an established order without an alteration in the standards within the field. Apple's encryption standards stood undiminished as did the established meaning system. With the restoration of equilibrium in the field, there was once again consensus about the relative positions of incumbents and challengers (Fligstein & McAdam, 2012). Apple managed to weather the crisis and retain its position as the incumbent by mobilizing the field against the external challenge. Crypto Wars 2.0 is considered to have ended with the withdrawal of the case against Apple. The legal battle ended without a conclusion and without establishing a legal precedent.

5.6 Conclusion

In this chapter we studied the standards contest in Crypto Wars 2.0 through the lens of an organizational field. Our exploration reveals that second crypto war had commenced five years prior to FBI's showdown with Apple. The law enforcement agencies articulation of the "going dark" issue in 2011 had sown the first seeds of discontent and once again highlighted the stalemate over encryption. This chapter found the Snowden revelation to be an exogenous shock to the *US Smartphone OS Encryption Field*. The event in 2013 had a direct impact on the law enforcement field but because of its proximity and dependence to the encryption field, the ripple effect penetrated the encryption field, prompting Apple to preemptively enhance its standards of encryption in the latest version of its OS (iOS 8). It was this radical change in encryption that

once again ignited the “going dark” debate in 2016 when Apple declared it couldn’t assist FBI with the unlocking of an iPhone in the San Bernadino case. Faced with an onset of crisis, this chapter examines Apple’s strategic resistance as an incumbent. The episode of contention made Apple undertake a mobilization process in which it not just rallied the entire encryption field but also “appropriated” the narrative on privacy rights and subsequently transformed the court case into a public debate of national proportions.

The next chapter performs an analysis of the key finding and insights of chapters 4 and 5 and present a comprehensive comparative table of Crypto Wars 1.0 and 2.0. It then proceeds to offer policy recommendation based on the findings. The chapter concludes by articulating the limitations of the thesis and laying down future research agenda.

Chapter 6: Analysis and Policy Recommendations

6.1 Introduction

The FBI vs Apple court case in February 2016, pushed encryption technology back into the headlines and reignited the privacy versus national security debate. The legal battle in the courtrooms of California and on Capitol Hill bore the contours of the stalemate between law enforcement agencies and technology companies. While FBI's demands for exceptional access into encrypted devices are made in the interest of national security, technology companies like Apple have campaigned for stronger encryption to ensure the protection of privacy rights of users. Encryption lies at the heart of this debate and has been the bone of contention between the two parties for over 25 years and counting.

This paper conceptualizes the stalemate as a standards issue and hypothesized that the stalemate arose from an acute standards vacuum, both in policy and technology. To that end, this paper states that the disagreements between law enforcement and technology industry is essentially a disagreement on encryption standards. Both parties, with opposing motivations, seek to establish their standards in order to benefit from them. The paper also seeks to uncover and unpack the kind of standards proposed by both sides during each of the Crypto Wars. By doing so, the paper explores the policy as well as technical standards of the government and technology companies. This study employs an organizational field framework to analyze both the wars with a common denominator. It also enables us to identify and define the field within which the actors operate, position and interact to set the agenda for encryption in communication devices. By identifying the encryption field of action we can also identify other fields that affect the encryption field as well as capture the broad environment within which the field is nested.

In chapters 4 and 5 we explored Crypto Wars 1.0 and Crypto Wars 2.0 respectively. Employing the organizational field framework, we examined the tension between the various actors, namely the incumbent actors and the challengers. We also took into account the effect of proximate, dependent and state fields upon the encryption fields. Standards formed the language of interaction between actors in the fields. Building on chapters 4 and 5, chapter 6 performs an analysis of the previous two chapters and presents its key findings and insights. By explaining the behavior of the actors and the fields, these findings offer new insights into the Crypto Wars and the prevalent stalemate. This chapter provides a comprehensive comparative table of the two Crypto Wars, which highlight the policy and technical standards proffered in each iteration of the wars. Next, based on the findings and insights, the chapter proceeds to offer preliminary policy recommendations for the future.

6.2 Analysis of Key Findings

6.2.1 Link of Continuity between Crypto Wars 1.0 and 2.0.

The paper establishes a link between Crypto Wars 1.0 and Crypto Wars 2.0 by conceptualizing both as part of the same organizational field. While the events of Crypto Wars 1.0 transpired within the *Commercial Hardware Encryption Field*, Crypto Wars 2.0 was a function of the turbulence in the *US Smartphone OS Encryption Field*. Both these fields exist as sub-fields of the Commercial Encryption Field.

Indeed, one of the key findings of the paper reveals that the standards that were established at the end of the first Crypto War in 2000 are seen to have been strengthened in the second iteration of the "war" a decade later. Indeed, it was this cumulative strengthening that led to the FBI complaining about "going dark". The primary standards resolution were

a. **The prohibition of "backdoors" into communication and computation devices**. The Clipper Chip followed by the Escrowed Encryption Standard (EES) were deemed counter-productive to the essence of encryption and abandoned by the year 2000.
b. **The abolition of licenses to export cryptography for commercial use.** Strict restrictions on the export of cryptography had prevailed since the cold war era and were eventually done away with under intense pressure from technology companies.
c. **No limitations on the key-length of crypto tools.** Encryption keys had been limited to within 56-bits to ensure they could be cracked by the intelligence and law enforcement bodies. The removal of limitations meant companies could create strong, internationally competitive products and US citizens could have access to strong encryption.
d. A general consensus that **government should not interfere in standards setting** and instead let competition in the open market decide their course.

We do observe that each of the above mentioned standards that were adopted at the beginning of the new millennium were intact during the onset of a new crypto war a decade later. Moreover, they appear to have been strengthened as standard key-lengths have expanded to up to 256-bit and encryption penetrated to a wider variety of devices and applications. This observation contextualizes the FBI vs Apple case as a part of the Crypto Wars canon and places both the "wars" along the same continuum.

6.2.2 Identifying the Standards Gap

This finding serves as the most significant among the findings in the paper. The thesis had commenced with the research question about the standards gap that contribute to the stalemate. The analysis reveals a sharp contrast in motivations of law enforcement and the technology community in proposing encryption standards. The essence of the finding lies in the fact that the

government did not take into account the market forces in its standards. Despite vociferous calls for exceptional access, the FBI's appeals failed to compel Apple to scale back its encryption standards. This mirrored the eventual outcome of the 1990s as well where the imposition of an escrow aided "backdoor" ultimately had to be sealed off.

As our examination of standard setting in the encryption field revealed, this is simply because "backdoors" are contrary to the forces of the market. In a field that is driven by competition and thrives in an open market, having a provision for exceptional access reduces the commercial viability and thereby the competitiveness of the crypto product. We have explained earlier the advent of crypto tools as a high value commercial entity. In the light of this reality, calls for backdoors can be characterized as counter-intuitive. Therefore, the standards gap exists in the perception of the nature of the encryption field and the forces that drive the creation of standards. While technology industry standards are based squarely upon the rules of market-driven compatibility standards, government standards ignore competition, market and network externalities as factors.

This (identify what this is) pertains to the question of motivation of the two sides. It is established that the organizational fields of interest to us in each of the "wars" was commercial in nature. Hence, the technology companies that operate within it as actors conceptualize standards as strategic commercial entities. Indeed, as laid down by the rules of compatibility standards, actors invest in a standards contest so that they can maximize profits from the standard. To that end, actors devote considerable resources in backing a standard that they hope will win a standards contest. Once a standard is established, actors can recover their investments and profit from it. Moreover, in a given field, standards also facilitate co-ordination and increase efficiency.

The standards proposed by the NSA and the FBI, on the other hand, arose from a different motivation. This paper shows that the government's standards were motivated not by monetary gains but access to communications and data. By controlling encryption standards, the NSA and the FBI hoped to maximize their profits from it by retaining unfettered access to data that would otherwise "go dark" through strong encryption. By engaging in a standards contest in Crypto Wars 1.0 from this perspective, the NSA ignored the commercial currents that drive the field. Therefore, by imposing its standards of key escrow, the NSA may have served its interests but ignored the reality that the field it was fighting a standards war in was guided by a different set of interests. Similarly, the FBI's attack on the *US Smartphone OS Encryption Field* through a demand for exceptional access would be beneficial for the FBI but harmful for the encryption field.

It is no surprise, then, that government standards could potentially alter the nature of the encryption field by undermining its true motivations. Thus, the standards vacuum in Crypto Wars 2.0 as well as Crypto War 1.0 was created by this fundamental difference in perceptions of "benefitting from a standard".

6.2.3 Role Reversal for the Government in the Encryption Field

A standards analysis of the Crypto Wars through an organizational field framework has revealed the nature of the government's role in the two "wars". In Crypto Wars 1.0, the NSA played the role of an active incumbent. However, in Crypto Wars 2.0, the FBI behaved as the challenger. This reversal of roles in the battle over encryption reflects the position from which the government approached the two "wars" and the bargaining power they had in it. An incumbent has been shown to possess a greater bargaining power in defining the rules of the field and relation of actors within it. The rules of the game are dictated by standards. A challenger,

though, as the name suggests, can mount a challenge to the rules set by the incumbent and offer an alternative institutional order and meaning system within the field (Garcia, 2004). The resources, allies in proximate fields and rules tend to be heavily stacked in favor of the incumbent.

In Crypto Wars 1.0, despite not having a commercial stake in the encryption field, the analysis revealed that the NSA had virtually hijacked the *Commercial Hardware Encryption Field*. It did so by appropriating AT&T's commercial encryption device – TSD 3600 D. Our examination of the field reveals that the NSA effectively placed itself as an incumbent by virtue of its prior monopoly of crypto tools till the 1980s before the civilian demand for encryption exploded. While the NSA actually did manage to impose its standards for about a decade through its privilege as incumbent, Crypto Wars 2.0 tells a different story. The FBI could only challenge the standards put in place by incumbents like Apple. Moreover, unlike the NSA, the FBI had no role as an actor inside the encryption field. Our exploration of Crypto Wars 2.0 revealed that the extent of FBI's impact on the proximate *US Smartphone OS Encryption Field* were the bouts of instability it effected through its challenges from the broader environment.

An important aspect of this finding lies in the fact that in both the avatars the essential demand of the government has remained the same. As incumbent and as challenger, the government's demand has primarily been the provision of a backdoor for exceptional access. However, while it did propose an alternative standard in the first edition of the war, it offered none during its second iteration. In order to re-orient the flow of resources in a given field, "the challenger must not simply compete for resources based on new forms of practices but must reinterpret current practices in the light of an alternative institutional logic" (Mohr, 2003 as cited in Garcia, 2004). Indeed, this sentiment is echoed by Abelson et al., (2015) in their statement,

"The current public policy debate is hampered by the fact that law enforcement has not provided a sufficiently complete statement of their requirements for technical experts or lawmakers to analyze". They posit that the closest the FBI has come to stating an alternative requirement was in October 2014, when FBI director, James Comey, stated "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. We are completely comfortable with court orders and legal process" (2014, as cited in Abelson et. Al, 2015).

6.2.4 Future Prospects: An Uneasy Equilibrium but a Strong Incumbent

A critical study of Crypto Wars 2.0 from an organizational field perspective has shed some light on the future prospects of the field. As exposed by the Snowden revelations (2013) followed by the FBI's legal challenge (2016), the stability of the *US Smartphone OS Encryption Field* remains susceptible to external shocks. However, Apple remains a strong incumbent with a proven record of weathering destabilizing attempts from proximate fields and its broader environment.

Unless the government directly intervenes through legislative action and enacts laws, this paper finds that the current encryption standards established by Apple will continue to serve as the dominant rules of the game for the *US Smartphone OS Encryption Field*. This brings us to our hypothesis stated in chapter 5:

Hypothesis: The Department of Justice can cause an episode of contention within "US Smartphone OS Encryption Field" but cannot alter its nature.

Our analysis of the *US Smartphone OS Encryption Field* has shown that the field has been at the receiving end of a number of exogenous shocks from its broad environment, which according to

Fligstein and McAdam (2012) is a "source of routine, rolling turbulence". Indeed, the legal challenge mounted on Apple by the Department of Justice's decision to move court in order to compel Apple's assistance in the San Bernadino case is one such example. However, the analysis reveals that this particular destabilizing change to the field did assume the form of a crisis. The onset of crisis, marked by an "episode of contention" in the field, was evident in the mobilization process undertaken by Apple to restore the stability of the field. The FBI vs Apple court case presented an assault on the stability by undermining the established standards of the field but was tackled by the mobilization of the entire encryption field and other dependent and proximate fields comprising actors from the technology industry and Silicon Valley. Ultimately, by withdrawing its motion in the court, the Department of Justice brought a sudden but voluntary end to the episode of contention, thus leaving the nature of the field intact.

Therefore, through its mobilization process and marshalling of resourced during the episode of contention, Apple, as the incumbent, performed its role in the field by restoring stability.

Table 1: Comparative table of Encryption Standards

		Crypto Wars 1.0	Crypto Wars 2.0
	Incumbent/ Initiative	**NSA (Government)**	**Apple**
POLICY STANDARDS	Device	Fixed line telephones	Smartphones
	Device type	Hardware	Software
	Volume of data	Voice conversation	Texts, pictures, call history, contacts, e-mails, notes
	Field type	Early formative stage	Established with defined actors
TECHNICAL STANDARDS	Encryption type	Key Escrow	Keys only with user
	Key Length	64-bit (Clipper Chip)	256-bit
	Encryption standard	Escrowed Encryption Standard (EES)	Advanced Encryption Standard (AES)
	Adoption	Voluntary	Default
	Backdoor	Yes	No
	License for Export	Yes	No
	Proprietary	Yes	Yes (iOS 8) No (Google Android)
	Interoperability	No	No (Apple) Yes (Google)

6.3 Policy Recommendations

The analysis of the encryption stalemate from a standards perspective has enabled us to understand the nature of the crypto war landscape as well as the relational dynamics between law enforcement and technology companies. Exploring the standards through an organizational field framework has revealed novel insights that inform our understanding of the contours of the encryption field environment, the actors, the relation among them, the structure of the fields and the dominant meaning systems that govern interaction.

In this context, the paper has found the encryption field to be a well-defined field with clear demarcations of incumbents, challengers and internal governance units. This is the case with the encryption field as well. We have charted the evolutionary course of the field's formation and development. An analysis of the crypto field revealed a number of sub-fields, one of which is the *US Smartphone OS Encryption Field* which is concerned with the encryption of data at rest. The FBI vs Apple battle was once again a contest over encryption standards, which effected potentially destabilizing changes in the field. While incumbents of the field like Apple has advocated for strong encryption to protect the privacy rights of Americans, the FBI has been vociferous in its demand for exceptional access in the interest of national security. This section offers policy recommendations based on our analysis, insights and findings to offer best practices and a way forward for tackling this enduring policy stalemate.

6.3.1 Moving Forward in a Post Crypto Wars 2.0 Environment

It has been a year since the FBI vs Apple case ended in March 2016. Moving forward, any attempts to alter the incumbent standards of encryption is likely to be untenable. This paper finds that weakening encryption standards would be counter-productive to both security and

privacy. This scenario will lead to increased costs by imperiling massive amounts of sensitive data and communications to attacks from malicious actors. Since the end of the first Crypto War, the internet has become a ubiquitous platform in our daily lives and a staggering amount of activities have been digitized. Therefore, even though the fundamental debate on privacy versus national security remains the same across the two Crypto Wars, what has undeniable changed is the scale and scope of systems reliant on strong encryption.

As revealed by standard setting in the encryption field, the government and its agencies should not intervene in standard setting in this arena. Not only will it provoke destabilizing changes within the field, which will require considerable resources in restoring the stability of the field once again but is also likely to stifle competition in an industry that sets its standards in response to increasing demand for encryption. Data flows across networks with little regard for national borders. If US encryption products are rendered weak, consumers will simply move to other non-US products that satisfy their demand for strong encryption. Additionally, the Encryption Working Group has observed in its year-end report (2016) that compromising encryption standards might also provide incentives for larger companies to move operations out of the US and into a country with a favorable legal environment. This will result not just in economic losses for the US but will law enforcement and intelligence will lose access to everything in the company's possession regardless of whether they are encrypted.

Given that law enforcement and encryption fields are characterized as proximate, there is scope for greater co-operation as well. The private sector can help law enforcement at state and local levels in technological capacity building. By fostering greater cooperation, law enforcement agencies can be brought up to speed with ways to leverage the vast amount of unencrypted data for investigate purposes.

6.4 Limitations

This paper represents an initial approach to conducting a standards based research of the Crypto Wars. While it presents a novel perspective to a decades-old issue and offers unique insights into the stalemate as well as the FBI vs Apple case, there are a few limitations that weigh upon the research. *First*, encryption as a technology is based upon mathematics and algorithms. While the paper delves deep into primary source documents and critically analyses policy perspectives, it provides limited insights into the esoteric technical aspects of encryption. Mathematics, which constitutes the nuts-and-bolts of encryption architecture does not inform the analysis performed in this paper.

Second, the framework used in this paper may be subject to criticism for being tailored to the eventual outcome of each of the crypto wars. The fact that the government failed in its endeavors to win a standards contest in both versions of the "war" may have colored the analysis to highlight the failures. This paper preemptively responds to this criticism by asserting that while it acknowledges the limitations in scope of the sociological framework, an organizational field perspective provides an abstract and generic framework into which any organization, industry or society can be viewed as a field. Therefore, the encryption fields that have been analyzed have objectively fit the framework.

6.5 Future Research Agenda

This paper has picked proverbial pebbles on the beach while the rapid technological advancements in cryptography and the internet ensures that a vast ocean of research opportunities lie ahead. The subject of this study is one that is constantly evolving and future research endeavors can contextualize developments after March 2016 along the same continuum of Crypto Wars 1.0 and Crypto Wars 2.0. Given that a tenable solution to the stalemate is still a

distant reality, this paper anticipates numerous important developments in the encryption debate as well as the larger privacy versus national security debate. The opening up of new avenues of unencrypted data such as in the Internet of Things (IoT) and cloud services means law enforcement could enhance its technological tools to exploit their potential. This translates into many new channels of research within the encryption fold. Moreover, this same subject can be interpreted through a deeper discussion of the mathematical aspects of encryption and standards.

This paper has combines two fields – standards and encryption – to offer a unique approach. Future studies can benefit from a collaboration of scholars from the two fields to carve out newer perspectives.

Bibliography

1. A complete guide to the new 'Crypto Wars' (2016, April 26). Retrieved from http://www.dailydot.com/layer8/encryption-crypto-wars-backdoors-timeline-security-privacy/
2. Abelson, H. "., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Specter, M. A., . . . Landau, S. (2015). Keys under doormats. *Communications of the ACM Communication. ACM, 58*(10), 24-26. doi:10.1145/2814825
3. Blaze, M. (1994, April 20). *Protocol Failure in the Escrowed Encryption Standard* [Scholarly project]. In *Www.crypto.com*. Retrieved February 01, 2017, from http://www.crypto.com/papers/eesproto.pdf
4. Blaze, M. (2012). *Key Escrow from a Safe Distance: Looking Back at the Clipper Chip* (Rep.). http://www.crypto.com/papers/escrow-acsac11.pdf
5. Borger, J., Ball, J., & Greenwald, G. (2013, September 06). Revealed: how US and UK spy agencies defeat internet privacy and security. Retrieved April 05, 2017, from https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
6. Busch, L. (2011). *Standards: Recipes for reality*. Cambridge, MA: MIT Press.
7. Comey JB. Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? Speech at the Brookings Institution, October 2014. https:// www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course
8. Cook, T. (2016, February 16). Customer Letter. Retrieved April 05, 2017, from http://www.apple.com/customer-letter/

9. D., Wilson, A., & Bankston, K. (2015, June). Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s. *Open Technology Institute - Cybersecurity Initiative*.
10. Diffie, W., & Landau, S. E. (2010). *Privacy on the line: the politics of wiretapping and encryption*. Cambridge, MA: MIT Press.
11. Edgar, T. (2016, March 19). Apple v. FBI Shows That Lawyers and Tech Speak Different Language on Privacy. Retrieved March 17, 2017, from https://lawfareblog.com/apple-v-fbi-shows-lawyers-and-tech-speak-different-language-privacy
12. Finklea, K. (2016, February 18). Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations. *Congressional Research Service*.
13. Fligstein, N., & McAdam, D. (2012). *A theory of fields*. New York: Oxford University Press.
14. Froomkin, A. Michael (1996) "It Came from Planet Clipper: The Battle Over Cryptographic Key "Escrow"," University of Chicago Legal Forum: Vol. 1996, Article 3. Available at: http://chicagounbound.uchicago.edu/uclf/vol1996/iss1/3
15. Garcia, D. L. (2004). Standards for Standards Setting: Contesting the Organizational Field. *Standards Edge*.
16. Garcia, D. L. (2016). The Evolution of the Internet: A Socioeconomic Account. *Handbook on the Economics of the Internet*, 529-552. Retrieved March 15, 2017.
17. Garcia, D. L., Liecky, B. L., & Willey, S. (2013). Public and Private Interests in Standard Setting: Conflict or Convergence. Retrieved from

https://blogs.commons.georgetown.edu/cctp-644-fall2015/files/2015/09/Wk2-Public-and-Private-Interests-in-Standard-Setting-Conflict-or-Convergence.pdf.

18. Greenwald, G., & MacAskill, E. (2013, June 07). NSA Prism program taps in to user data of Apple, Google and others. Retrieved April 05, 2017, from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
19. Grewal, D. S. (2008). *Network power: The social dynamics of globalization*. New Haven: Yale University Press.
20. Grimmelmann, J. (2015). *Internet law: Cases and problems*. Lake Oswego, OR: Semaphore Press.
21. Grindley, P. (1995). *Standards strategy and policy: cases and stories*. Oxford: Oxford University Press.
22. Hao, L. (2014). *The Paradox of Standard Setting in Globalized Agri-Food Production System*. UMI.
23. Horan, T. M. (2016). *Surveillance Versus Privacy, with International Companies Caught in Between* (Rep.). American Enterprise Institute. www.aei.org
24. Jamil N. Jaffer & Daniel J. Rosenthal, Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge, 24 Cath. U. J. L. & Tech (2016). Available at: http://scholarship.law.edu/jlt/vol24/iss2/3
25. Kehl, D., Wilson, A., & Bankston, K. (2015). *Doomed to Repeat History: Lessons from the Crypto Wars of he 1990s* (Rep.). New America.
26. Kelion, L. (2013, July 01). Q&A: NSA's Prism internet surveillance scheme. Retrieved April 05, 2017, from http://www.bbc.com/news/technology-23051248

27. Landau, S. E. (2013). *Surveillance or security?: the risks posed by new wiretapping technologies*. Cambridge, MA: MIT Press.

28. Levy, S. (1994, June 11). Battle of the Clipper Chip. Retrieved April 05, 2017, from http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all

29. Levy, S. (2002). *Crypto: How the code rebels beat the government-- saving privacy in the digital age*. New York: Penguin Books.

30. Newman, L. H. (2014, September 18). Here's How to Keep Apple From Sharing Your iPhone Data With the Police. Retrieved April 05, 2017, from http://www.slate.com/blogs/future_tense/2014/09/18/if_you_use_a_passcode_in_ios_8_apple_won_t_be_able_to_give_your_personal.html

31. Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford Law Books.

32. Perlroth, N., Larson, J., & Shane, S. (2013, September 05). N.S.A. Able to Foil Basic Safeguards of Privacy on Web. Retrieved April 05, 2017, from http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&_r=0

33. Privacy. (n.d.). Retrieved April 05, 2017, from http://www.apple.com/privacy/

34. Rauch, J. E., & Casella, A. (2001). *Networks and markets*. New York: Russell Sage.

35. Schmidt, S. K., & Werle, R. (1998). *Coordinating technology: Studies in the international standardization of telecommunications*. Cambridge, MA: MIT Press.

36. Schneier, B. (n.d.). *Data and Goliath: The hidden battles to collect your data and control your world*.

37. Schuetz, D. (n.d.). A (not so) quick primer on iOS encryption. Retrieved April 05, 2017, from https://www.darthnull.org/2014/10/06/ios-encryption

38. Shapiro, C., & Varian, H. R. (2010). *Information rules: a strategic guide to the network economy*. Boston, MA: Harvard Business School Press.

39. Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. New Haven: Yale University Press.

40. Staff, D. T. (2016, April 03). The Apple vs. FBI showdown is over! Here's a full timeline of events. Retrieved April 05, 2017, from http://www.digitaltrends.com/mobile/apple-encryption-court-order-news/

41. Streitfeld, D., & Hardy, Q. (2013, June 09). Data-Driven Tech Industry Is Shaken by Online Privacy Fears. Retrieved April 05, 2017, from http://www.nytimes.com/2013/06/10/technology/data-driven-tech-industry-is-shaken-by-online-privacy-fears.html

42. Szoldra, P. (2016, September 16). This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks. Retrieved April 05, 2017, from http://www.businessinsider.com/snowden-leaks-timeline-2016-9

43. Timberg, C. (2014, September 18). Newest Androids will join iPhones in offering default encryption, blocking police. Retrieved April 05, 2017, from https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/?utm_term=.5a1c0b0ba7d4

44. Upton, F., & Goodlatte, B. (2016). *Encryption Working Group Year-End Report* (Rep.). Encryption Working Group.

45. Weitzner, D. J. (2016, March). The Encryption Debate Enters Phase Two. Retrieved from https://www.lawfareblog.com/encryption-debate-enters-phase-two

46. White House Clipper Statement (4/16/93). (n.d.). Retrieved April 05, 2017, from https://www.epic.org/crypto/clipper/white_house_statement_4_93.html

47. Why can't Apple decrypt your iPhone? (2016, July 28). Retrieved April 05, 2017, from https://blog.cryptographyengineering.com/2014/10/04/why-cant-apple-decrypt-your-iphone/

www.newamerica.org

48. Zittrain, J. (n.d.). Don't Panic: Making Progress on the Going Dark Debate. Retrieved from https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.