Encryption and Globalization

Peter Swire & Kenesa Ahmad*

Note to Reader: This document is a discussion draft. Some pieces are relatively polished, but others are not. The overall goal is to create a law review article, suitable for reading by policymakers globally, on encryption and globalization. It should be accurate in the eyes of varied audiences, including cryptographers, business people in the field, government officials, and lawyers.

The overall idea is to have a document that brings crypto policy up to date after its low profile since 1999. Many different countries are considering crypto regulations, notably India and China with their large populations and important economies, but other countries as well. Most policymakers today are not very familiar with the policy issues debated in the U.S. in the 1990's, and new issues arise as encryption policy becomes globalized.

A basic conclusion is to stress the importance of strong encryption for hardware and software used in the global Internet. A second theme, which will be discussed in a revised policy discussion in Part VI, is to examine how this conclusion about strong encryption supports caution on CALEA-style regulation; to the extent CALEA-style regulations are promulgated, there are nonetheless strong arguments, developed here we believe for the first time, to support strong encryption for Internet communications.

The table of contents provides an outline of the discussion. Apologies to the readers not to have each piece more fully developed. Comments to the readers are given in brackets: "[" and "]".

For readers with a good background on wiretaps and encryption, the highest priority pieces to read are likely to be:

Part IV: the arguments for why strong encryption is essential to cybersecurity and the "least trusted country" argument.

Part V: the "going dark" vs. "golden age of surveillance" debate; the discussion of likelihood of back doors (although the section requires a stylistic rewrite); the international trade discussion.

Part Vi: this part is written in especially preliminary form; as noted at the start of Part V, the question is whether the 2x2 matrix is a useful analytic tool; more work is needed to explain how the matrix would apply to policy issues; more work is also needed on MLATs and other possible improvements to lawful access to communications

---

* Peter Swire is the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University. His work on this article draws on his experience as Chief Counselor for Privacy in the U.S. Office of Management and Budget from 1999 to early 2001. In that role, he chaired the White House Working Group on Encryption in the period that culminated in the September, 1999 announcement that the Clinton Administration would support strong encryption. In 2000, he chaired a White House Working Group on Updating Wiretap Law for the Internet Age, which resulted in an administration legislative proposal. In 2011, Swire visited India to meet with public officials and the private sector on encryption issues.

Kenesa Ahmad received her JD from the Moritz College of Law of the Ohio State University, where she served as an editor of the Ohio State Law Journal, and received her LLM from Northwestern University Law School. She is now a Legal and Policy Associate with the Future of Privacy Forum.

For financial support, the authors thank the Future of Privacy Forum, Intel, and the Moritz College of Law of the Ohio State University. The authors also thank [insert names] for their assistance in this project.

Readers are specifically encouraged to provide suggestions for current uses of encryption in modern computing and telecommunications, or sources that cover this.

I. A Short History of Wiretaps for Phone and Data in the U.S.

To understand the importance of encryption today it is helpful to consider how wiretap technology has evolved in recent decades. Originally, wiretaps were conducted through copper telephone wires. In this scenario, Alice would make a phone call to Bob, as illustrated in Figure 1.[1] [Note to reader – all figures in this discussion draft are in the Appendix.] The police or other wire-tapper would touch a separate copper wire to the copper wire between Alice's house and her local telephone company switch. Through the process of induction, the sound waves traveling through the circuit between Alice's phone and Bob's phone could be listened to through the wiretap. This was a fairly simple process, merely connecting a listening device (the wiretap) to the circuit carrying sound waves between phones.

The approach to wiretapping shifted dramatically with the widespread adoption of fiber optic lines in the early 1990s. Figure 2 illustrates this shift in technology. In this situation, Alice is once again making a telephone call to Bob. This time, however, glass fiber connects Alice to her local telephone switch. If the police or other wire-tapper touches a copper wire or to the glass fiber between Alice's house and the local switch, the wire-tapper ends up with a distinctly disappointing result – no sound travels to the wire-tapper. This switch from copper wires to fiber optics in telephony thus created a difficult challenge for law enforcement agencies in carrying out the lawful interception of information. The answer to this problem was the enactment of the Communications Assistance for Law Enforcement Act (CALEA) in 1994.[2] The major theme in CALEA was to ensure that law enforcement surveillance capabilities remain intact during the move from a copper-wire phone system to digital networks. Under CALEA, telephone companies, telecommunication service providers, and manufacturers of telecommunication equipment were required to update their equipment, facilities, and services to ensure that they have built-in surveillance capabilities, so that law enforcement agencies could monitor transmissions in real time. In practice, this meant that the telephone call traveled from Alice's house to the local switch without being intercepted. Then, at the switch, the wiretap order could be implemented.

CALEA provided critical new tools for law enforcement and, in many ways, made wiretapping much more effective than before. Notably, CALEA made it far easier to implement wiretaps remotely. Instead of the police officer physically sitting outside of the target's house, CALEA-equipped FBI agents could retrieve a direct feed from the local phone company switch to the agent's office. Especially on hot or rainy days, this obviously made an agent's life more pleasant. Along with logistical advantages of CALEA wiretaps, a clear limit was written into the statute. The legislative compromise at the core of CALEA provided that new wiretap ready requirements applied to voice networks but did not apply to internet protocol communications.[3]

---

[1] The names Alice and Bob were first publicly used by Ron Rivest for discussion of encryption implementations in the 1978 Communications of the ACM article presenting the RSA cryptosystem, and in A Method for Obtaining Digital Signatures and Public-Key Cryptosystems published April 4, 1977, revised September 1, 1977 as technical Memo LCS/TM82.

[2] CALEA 47 USC 1001-1010.

[3] The privacy advocacy community suffered a major rift during consideration of CALEA. The Washington office of the Electronic Frontier Foundation, headed by Jerry Berman, played a major role in negotiating the compromise that excluded CALEA requirements from the IP network. Other advocacy groups argued vehemently against having any requirements of wiretap readiness built into the phone networks. In the aftermath of this debate, Berman and his group left the EFF and founded the Center for Democracy and Technology, which has remained active in U.S. wiretap debates ever since.

Coincidentally or not, the exponential growth of the Internet began just as CALEA was enacted. During the 1990s, telephone companies were forced to submit new technologies to the FBI for review to ensure compliance with CALEA wiretap readiness requirements. By contrast, new Internet software and hardware technologies were being developed as the estimated number of users grew at an annual rate of X% from 1994 to 2000, when the estimated number of Internet users exceed 1 billion people.[4] It is hard to imagine attaining this level of growth if software and hardware providers had been subject to the same FBI clearance requirements as their voice network counterparts.

a. The Importance of Encryption for an Insecure Channel such as the Internet

As the Internet experienced rapid growth throughout the 1990s, the importance of strong encryption to its sustainability became increasingly apparent. Figure 3 illustrates this basic point. In this diagram, Alice is once again communicating with Bob. The difference, however, is that she is now sending Bob an e-mail through the Internet. The connection between Alice and her local Internet Service Provider (ISP) is quite similar to the connection between Alice and her local telephone switch. The crucial difference arises, however, in how the communication travels from Alice's ISP to Bob's ISP. The Internet was originally designed to enable communication even in the face of severe damage, such as that incurred during war. This resilience is possible through the availability of numerous nodes to receive packets of information from Alice's ISP and route them on towards Bob's ISP. Peter Huber has termed this the "geodesic network" in which each node of the Internet is analogous to the nodes of the geodesic domes pioneered Buckminster Fuller.[5] Figure 4 provides an example of a geodesic dome. In a geodesic network, there are innumerable paths between any two points in the network. If one route is blocked, the communication can simply travel through alternate nodes to arrive at the destination.[6] Although nation states have since developed a variety of ways to apply existing law to the Internet, the basic fact remains that an Internet network consisting of millions of nodes results in an exponentially larger number of paths possible between Alice and Bob.

The Internet that emerged during the 1990s, thus, was resilient against damage, and was open to enormous growth as new nodes continued to arrive online. The trustworthiness of those nodes, however, was completely unknown. In contrast with the telephone network, in which a small number of telephone companies controlled the vast bulk of calls, an astonishing number and variety of actors controlled the nodes within the Internet. Many of these entities were legitimate universities, companies or other organizations. However, there was no guarantee that communications would only travel through nodes operated by these legitimate organizations. For instance, communications traveling through nodes controlled by hackers or other criminals could be tampered with or copied and used in future cyber attacks. Communications traveling through insecure nodes operated by amateur actors were subject to attack from outsiders. Additionally, nodes could be operated by hostile foreign governments or by entities controlled by hostile foreign governments.

The systematic insecurity of the intervening Internet nodes is a fundamental reason why encryption became essential to the growth of the Internet. As commercial and government use of the Internet grew, it became impractical to allow communications to travel unprotected and to be intercepted by unknown and possibly malicious parties within the network. Consider financial transactions that could be intercepted by

[4] [Cite statistics]
[5] [Cite Huber, Geodesic Network report]
[6] Early Internet theorist Robert May popularized the slogan that "the Internet treats regulation as damage and routes around it."

criminals. These malicious parties could quite possibly steal payments intended for others, or make copies of the transaction order and cash in the order multiple times. Few would conduct serious business on the Internet if they believed that malicious parties could access and read their communications. Technical experts familiar with the problem argued vehemently for strong encryption so that personal communications and business transactions would be protected. As discussed below in Section __, technology industry leaders, civil right activists, and technical experts alike recognized the need for strong encryption on the Internet. Moreover, this new generation of encryption was feasible and easy to deploy for many users.

II. Encryption Basics Relevant to the Legal and Policy Analysis

In order to understand the policy and legal issues discussed later in this paper, it is helpful to have a basic understanding of some encryption basics: private-key (or "symmetric") encryption; public-key (or "asymmetric") encryption; and major categories of how encryption is subject to attack.

A. **Private-Key or Symmetric Encryption**

Long before the advent of the Internet, there were numerous reasons to try to send messages in a format that only intended recipients could read and understand.[7] Since ancient days, military commanders sought mechanisms for communicating with allies without revealing secrets to enemies. Merchants used codes when sending commercially sensitive information to distant lands. The telegraph created a large new demand for encryption, because telegraph operators and others between the sender and recipient could otherwise read the message. The radio also encouraged development of encryption, because its broadcasts could be heard by both friends and enemies. A well-known example of encryption for use with radio was the Enigma encryption system used by the Germans during World War II, to communicate between radio towers in Europe and U-boats operating in the Atlantic Ocean.

A cryptosystem has three major elements: (1) an encryption mechanism, often a mathematical algorithm for turning plaintext (the original message) into ciphertext (the message in encrypted form); (2) a decryption mechanism, often an algorithm for turning ciphertext back into plaintext; and (3) a mechanism for generating and distributing keys. A cryptographic key has the same function as a key or combination for a physical-world lock. A physical-world lock has a standard blank, such as for a model of car, but each car key is cut slightly differently to fit a particular lock. Similarly, for the sorts of locks often seen in high school locker rooms, each lock has a different numerical combination.

To take a simple example, suppose that encryption happens by changing each letter in plaintext into a letter x spaces later in the alphabet. If x=2, then "a" shifts two letters to "c" and "b" becomes "d." Decryption happens by reversing the operation, so "c" becomes "a" and "d" becomes "b." In this example, the key is "2", showing how many letters to shift in the alphabet. In this example, there are 26 possible keys, because "a" can turn into any one of the 26 letters of the alphabet (including "a," which would leave the message in plaintext).

In this approach, Alice and Bob would use the same encryption algorithms for encoding and decoding the message. When Alice wished to send a message to Bob, she would wrap the plaintext message with an agreed-upon secret key. Upon receipt of the encrypted message, Bob would unwrap the message using the same private key. This approach is known as "symmetric" encryption, because the key is the same on both ends

[7] Useful histories of encryption include [insert cites].

of the communication. It is also known as "private key encryption," because the key has to remain private – secret -- to possible attackers while being known to Alice and Bob.

In this approach, it is critical to generate and share the key securely. It is true that users have often also sought to keep secret the encryption and decryption mechanisms. During World War II, for instance, the Germans tried to keep secret the physical workings of the Enigma machines, and Allied codebreakers made important progress when they were able to analyze captured Enigma machines. As discussed further below, however, encryption experts have long believed that the security of the overall encryption should depend on the secrecy of the key and not on secrecy of the rest of the cryptosystem. Major breakthroughs on Enigma came when the Allies captured German codebooks that provided the keys used for particular dates.[8] In order to share the symmetric keys, the Germans printed codebooks placed on each U-boat and other naval vessels. German officers were supposed to destroy the codebooks if the vessel was going to be captured. Once the Allies captured some codebooks, however, large swathes of German communications became readable. Historians have concluded that these and other encryption breakthroughs may have shortened the length of World War II by two years or more.[9]

B. **Public Key or Asymmetric encryption**

A new and in many ways radical approach to encryption developed during the 1970's and became widespread on the Internet in the 1990's. This "public key" or "asymmetric" encryption was derived from the Diffie-Hellman multi-user encryption concept.[10] Its best-known cryptosystem became known as RSA based on the names of cryptographers Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman.[11]

Instead of sharing the same key between Alice and Bob, asymmetric encryption uses two different keys for encryption and decryption. In a public key system, the recipient Bob has a public key that everyone can access. Bob also has a secret, private key that allows him to decrypt these messages. Though Bob publishes his public key he does not tell anyone his private key, not even Alice. When Alice wants to send Bob a message, she wraps the message in his publically available key, and then sends it in encrypted form to her ISP where it travels through the network to Bob's ISP and eventually reaches Bob. Upon receipt, Bob uses his private key to unwrap the message and read its plaintext contents. Figure 5 illustrates the structure of a public key encryption system. If Bob wants to reply back to Alice, he wraps his message in her public key and then she unwraps it using her private key.

The complicated mathematics of an asymmetrical encryption algorithm are beyond the scope of this paper, but the basic concept behind the public-key system is simple.[12] The process depends on a "one way function," a calculation that is much, much easier in one direction than it is to reverse. An analogy would be a grade school child who has learned multiplication but not yet learned long division – multiplying two numbers

[8] http://www.militaryhistoryonline.com/wwii/atlantic/enigma.aspx.
[9] English historian Sir Harry Hinsley, Bletchley Park, http://www.cl.cam.ac.uk/research/security/Historical/hinsley.html
[10] Diffie Hellman stuff
[11] Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM 21 (2)
[12] See www.rsa.com for more information on the mathematical process of deriving private and public keys using the RSA algorithm.

is fairly easy, but the child doesn't know how to divide the resulting number into its factors. The premise of the RSA algorithm is that it is easy to multiple two large prime numbers but very difficult to use the product of those numbers to reverse the process and determine what those original prime numbers are.[13]

This simplified explanation of public key encryption leads to two important themes for encryption and the global Internet. First, the public key approach directly addresses the most glaring weakness of the private-key approach. It allows people to send messages to each other without first having to securely share a secret key. Instead, all communications to Bob are wrapped up with the same, publically available key. This public-key approach thus addresses the traditional distrust for shared secrets among cryptographers, who often quote Benjamin Franklin in saying that "three can keep a secret if two of them are dead."[14]

A second and related advantage of public key encryption is that the approach can scale to very large numbers of users. With the old symmetric key approach, the risk of compromise increased each time that one more unwanted party, or U-boat, gained access to the key. By contrast, the public key approach simply requires publication of one additional public key when a new user wishes to participate. The addition of the incremental user does not change the risk for existing users.

C. **Categories of Encryption Vulnerabilities**

Although public-key encryption helps greatly with distribution of keys, any form of encryption is subject to three basic categories of attack: 1) brute force attacks; 2) attacks that are more efficient than brute force; and 3) attacks assisted by a flaw known to the attacker, or "backdoors." Understanding these categories of attacks is directly helpful to current policy debates about encryption.

1. Brute force attacks. In a brute force attack, the code breaker's computer tries every possible key combination in order to find the one that will work. That is why key length is so important to the policy debates about encryption. The attacker can quickly try every combination for a short key length, but lacks the computational power to break a long key.[15]

With apologies to readers who don't like mathematics, understanding key length is much easier with a reminder of the basics of exponents. Key length is measured in bits, where each digit is either zero or 1. A 10 bit key has [2 to the tenth] combinations, or 1024 possible keys. A key length of 11 doubles the number, or 2048 keys. And [2 to the 12th] equals 4096 keys. This example shows how adding to the length of keys produces an exponential growth in the number of combinations. Sometimes people think that going from 10

---

[13] This is an example of a one-way function, a mathematical operation that takes little computational effort to execute but a vast amount of effort to reverse, if reversal is possible. For a concise explanation of one-way, or cryptographic, hashes, see __

[14] Ben Franklin

[15] Having a long key certainly does not guarantee that an encrypted message is secure. There can be other flaws in the cryptosystem, or implementation of the cryptosystem can be flawed in numerous ways. The point here is that having a short key does mean that attackers can easily read the message.

As an analogy, imagine that the attacker is trying to get through a door into a room. A long key is similar to a steel door – it is very difficult to get in the front door. A short key is similar to having a paper door – anyone can get in. And a steel door is useful but won't keep attackers out if a window is open or the wall is made out of flimsy wood. Long enough keys are thus necessary for security but not sufficient.

bits to 12 bits is a 20% increase, because 12 is 20% higher than 10. That is incorrect. Instead, going from 10 bits to 12 bits is a 400% increase, from 1024 combinations up to 4096 combinations. Going from 10 bits to 20 bits is not a doubling of the number of combinations; instead 20 bits has 1024 times more combinations than 10 bits.

This reminder about exponential growth is important to understanding brute force attacks. Current encryption law in India, written in 1999, has a maximum key length of 40 bits. This key length is trivial to break. Already in 1996, leading cryptography experts showed that a 40-bit key could be broken in five hours at a cost of equipment of $400.[16] Fifteen years later, computing speeds are massively greater, so a modern personal computer could break such a key in far less time. By contrast, standard banking transactions in the United States often use a key length such as 1024.[17]

Sufficient key length should not only be strong enough to defeat attacks today. Computing power and speed are increasing rapidly – Moore's Law states that the performance of microprocessors (and thus computing power) doubles roughly every 18 months.[18] Because many encrypted messages should remain private for a long period of time (e.g., medical records, personal emails), good practice is to use a key length strong enough to resist attack both today and in future periods where privacy of the message remains important.

Having a long key is important but in no way guarantees that an encrypted message is secure. There can be other flaws in the cryptosystem, or implementation of the cryptosystem can be flawed in numerous ways. The point here is that having a short key does mean that attackers can easily read the message. As an analogy, imagine that the attacker is trying to get through a door into a room. A long key is similar to a steel door – it is very difficult to get in the front door. A short key is similar to having a paper door – anyone can get in. And a steel door is useful but won't keep attackers out if a window is open or the wall is made out of flimsy wood. Long enough keys are thus necessary for security but not sufficient. Brute force attacks succeed against short keys, and long keys at least make security possible to achieve.

2. Improving on brute force attacks and the importance of peer review. An important category of decryption work is for attackers to try to improve on brute force attacks, in order to read the message in less time than needed for a brute force attack. A perfect encryption system would make the likelihood of each key be precisely the same. In that setting, on average, an attacker would have to try half of the total number of combinations in order to chance upon the correct key.[19] Suppose, however, that the attacker somehow found out that only even numbers would be used and no odd numbers. For a long key, this would still leave the attacker with numerous combinations to attempt. Importantly, however, the number of possible correct combinations

[16] Matt Blaze, Whitfield Diffie, et al., "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security," (Jan. 1996), available at http://www.schneier.com/paper-keylength.pdf.
[17] [cite] Mathematically, a key length of 1024 has [2 to the 984th] more combinations than a 40 bit key length.
[18] Moore's law, named after Intel co-founder Gordon Moore, is based on his 1965 prediction that the number of transistors on microprocessors would double approximately every 18 months and that this would continue for the foreseeable future. [Cite]
[19] The average number is half of the number of total combinations because occasionally the attacker will get lucky and have the key be in the first 1% of combinations and occasionally the attacker will be very unlucky and be in the last 1 % of combinations attempted. Those lucky and unlucky events have an average of (1+99)/2=50. That simple numerical example illustrates why random chance will lead to an average outcome of about 50% of the combinations.

would be reduced by half, and the average time to solve the problem would now be 25% of the time needed to test all the original combinations.[20] Any incremental reduction in disorder (i.e. reduction in randomness) reduces the time needed to find the correct key. Cryptologists thus often seek even partial solutions in order to reduce the randomness that masks the correct key.[21]

Cryptographers widely agree that it is extraordinarily difficult to create an algorithm that generates keys entirely randomly. Many encryption algorithms that have been proposed over time have been flawed, such as in the overly simplified example here, in which only even numbers are used in a key. As a leading cryptography text says: "There is no known way of testing whether a system is secure. In the security and cryptography research community … what we try to do is publish our systems and then get other experts to look at them…. Even with many seasoned eyes looking at the system, security deficiencies may not be uncovered for years."[22] Until a cryptosystem has withstood this public scrutiny and rigorous peer review, experts have considerable skepticism about its reliability and security. This is currently a major issue in connection with China's encryption algorithms, which, as described below, have been developed to date without significant public peer review. In addition, as also discussed below, having a good cryptosystem and long key length are not enough – many vulnerabilities can crop up at the implementation level, when the system is actually deployed in a broader information technology system.

3. Backdoors. Another category of vulnerabilities for encryption system is if a programmer intentionally creates a vulnerability. These intentional flaws are often called "backdoors." The image is that the front door may be securely locked, but someone who knows the place well can enter through a back door that seems locked but is easy to open.

Backdoors into communications systems can seem attractive to some stakeholders. For instance, a corporate system administrator might wish to retain access to all the data and communications in the system, to ensure that corporate policies are being followed.[23] More prominently in the encryption debates, law enforcement and national security agencies may wish to have a backdoor into telephone or data communications. CALEA notably requires the traditional telephone system to have a backdoor – to be designed to carry out wiretap orders. Law enforcement and national security agencies also have pushed to have access to encrypted communications, such as through limits on key length or the "key escrow" approach discussed below.

The Vodafone incident in Greece illustrates the security risks created by backdoors. In 2004 and 2005, the calls of the Greek Prime Minister and over 100 other high-ranking government officials were subject to

[20] The 25% figure results from: 1) the average time of 50% for all of the combinations; and 2) the fact that only half of those combinations are even. .5*.5=.25 and thus the average time to solve the key would be the time it takes to calculate ¼ of the total possible combinations.

[21] For those with a physics background the incremental likelihood of Id a key can be described as reducing entropy in the system. Maximum randomness is equivalent to complete entropy, or entropy = (1). Whereas incremental efficiency reduces entropy until at the extreme a solution that correctly identifies the key as zero entropy. Zero entropy means complete order, because the randomness of the result has been eliminated. End FN

[22] Niels Ferguson, Bruce Schneier, & Tadayoshi Kohno, Cryptography Engineering 13 (2d ed. 2010).

[23] For instance, system administrators in the U.S. often retain the ability to read emails sent on the system. Under U.S. law, emails on the corporate system belong to the corporation rather than the individual. [Cite]

illegal wiretaps. The perpetrators, illegally gained access to the legal interception capabilities built into the Ericsson software used to run the Vodafone network switching system. The perpetrators were never caught.[24]

Despite the attractiveness of backdoors for surveillance purposes, there are serious security risks to having backdoors. It is complex and extremely difficult to create a secure communications mechanism, such as strong encryption. It is even more difficult then to create a vulnerability that is usable by the "good guys," such as authorized law enforcement wiretappers, but not by the "bad guys," such as the perpetrators in Greece. The security risks caused by surveillance technologies is the central theme of an important recent book by cryptography expert Susan Landau, entitled "Surveillance or Security? The Risks Posed by New Wiretapping Technologies."[25] As Landau explains, the security holes created in the name of security and surveillance can easily pose greater risks than the benefits to the agencies from the information thus collected.

III. From the U.S. "Crypto Wars" to the New Global Encryption Debates

The United States government placed serious limits on strong encryption during the 1990's. After the intense policy debates often known as the "crypto wars," the Clinton administration shifted position in 1999, permitting the widespread use of strong encryption at home and abroad. Encryption as a public policy issue then almost entirely disappeared from view until very recently, when new developments in countries including India and China have revived many of the same issues hotly debated in the U.S. during the crypto wars.

A. The Crypto Wars

Prior to the 1990's, the National Security Agency (NSA) played a predominant role in U.S. encryption. As part of the Department of Defense, the NSA could fulfill two complimentary roles that have historically been essential to military operations. The first role was offensive - namely, the decryption of codes used by foreign forces or other targets of communications surveillance. The second role was defensive - to protect effective encryption used by the U.S. military, the rest of the U.S. government, and key industries that used encryption. After World War II and until the development of public key encryption, NSA regularly recruited the country's best cryptographers.[26] This changed as computer technology advanced and public key cryptography was developed in public, rather than being classified as a national security secret. Companies and individuals began to develop their own encryption systems outside of the NSA's control. As a result, law enforcement and national security agencies became increasingly concerned that the proliferation of private sector encryption would erode their ability to monitor criminals and foreign entities. They made numerous attempts to stifle the outside development of encryption.[27] By the end of the George H.W. Bush administration in1992, non-NSA encryption had become an important policy issue for national security policymakers.[28]

---

[24] Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair," IEEE Spectrum, July 2007, available at < http://spectrum.ieee.org/telecom/security/the-athens-affair>

[25] Susan Landau, Surveillance or Security? The Risks Posed by New Wiretapping Technologies (2011).

[26] The recruitment of talented young cryptographers has featured prominently in two popular movies. In "A Beautiful Mind," (2001) real-life mathematician John Nash was hired by the government to work on codes. In "Good Will Hunting," (1997) the fictional character played by Matt Damon was also recruited to use his cryptographic talents for the government, but he refused to be hired.

[27] This included the use of secrecy orders against researchers and the revocation of funding for outside encryption research. See Steven Levy, Crypto: Secrecy and Privacy in the New Code War (2001).

[28] Id.

1. Key escrow and Clipper chip. When President Clinton entered office, the ideas of "key escrow" and "Clipper chip" became the central battleground.[29] For the administration, key escrow appeared to provide a way to have strong encryption for ordinary communications while still giving access when needed to law enforcement and national security agencies. With key escrow, the government would permit widespread use of strong cryptosystems with long keys. That would mean effective protection against brute force attacks. The tradeoff, though, was that users of the strong encryption would need to keep their keys on file with the government – the keys would be in "escrow."[30] The government planned to establish two key-escrow data banks, to be run by independent entities, which would each hold part of the key.[31] When a proper court order existed for the communications of a suspect, the two key-escrow data banks would reveal their parts of the key to the agency carrying out the surveillance.[32] That agency could piece the two parts of the key together. It would then be able to read that suspect's communications, but other communications in the network would remain strongly encrypted and unavailable to the government agencies.

The Clipper chip was a specific chipset intended for use in voice communication equipment, but the term "Clipper chip" soon became shorthand for the much broader debates about key escrow and the use of strong encryption in communications. The Clipper chip used a data encryption algorithm called Skipjack, which was sharply criticized by many in the encryption community because it had not been peer reviewed.[33] Although the chip was not ever widely put into production, the idea was that a new telephone or other communications device would be given a key while in the factory. Each half of the key would be escrowed with a different entity, and the keys would be provided to a law enforcement or national security agency when the proper legal process existed. The agency could then decrypt all data transmitted by that particular telephone or other device.

Clipper chip was never put into practice on a meaningful scale. Manufacturers failed to warm to a government-designed chip that was controversial. The implementation had technical flaws, such as Matt Blaze's discovery in 1994 of ways to disable the key on the chip, so that the escrowed key would not work on

---

[29] In addition to the detailed history of the period in the Levy book, helpful sources for information about the 1990s encryption controversy are available from public interest groups that were active in the crypto wars: the Center for Democracy and Technology, http://www.cdt.org/crypto; and the Electronic Privacy Information Center, http://epic.org/crypto.

[30] Escrow is a legal term meaning "a deed, a bond, money, or a piece of property held in trust by a third party to be turned over to the grantee only upon fulfillment of a condition." Mirriam-Webster Dictionary, available at http://www.merriam-webster.com/dictionary/escrow. Applied to encryption, the key would be the piece of property held in trust by an escrow authority established by the U.S. government. The key would be turned over to a law enforcement or national security agency when a condition was fulfilled, the proper court order.

[31] The White House, Statement by the Press Secretary, April 16, 1993, available at http://epic.org/crypto/clipper/white_house_statement_4_93.html

[32] The use of the split key, held by two different entities, was intended to allay fears that a single data bank could be compromised by insider abuse or outside attack. The idea was that the key could only revealed by having access to two separate data banks, and collusion between the two data banks would be difficult.

[33] Skipjack was developed by the NSA and initially classified SECRET, so it could not be subjected to peer review. The algorithm was made public in 1998. [cite]

the phone's communications.[34] Perhaps most importantly, impassioned opposition developed, especially by leading civil liberties groups and many techies[35] – a vocal constituency who were in the midst of creating the revolution that was growing the Internet from its first commercial activities in 1993 to over a billion users by 2000.[36] To give a flavor of the opposition to revealing keys, consider a well-known quotation by John Perry Barlow, a founder of the Electronic Frontier Foundation: "You can have my encryption algorithm … when you pry my cold dead fingers from its private key."[37]

Key escrow continued to be government policy after the failure of the Clipper chip,[38] and leading encryption experts published a comprehensive critique of key escrow in 1997.[39] Because key escrow continues to be considered seriously in encryption debates today, currently in India, it is useful to highlight three dimensions of the critique. First, key escrow increases risks in operating an encryption system. As with any backdoor or intentional vulnerability, the system is now subject to a known attack rather than having the higher likelihood of security where no such known vulnerability exists. In particular, the storage of the keys creates "high-value targets for criminals or other attackers."[40] In addition to possible abuse by insiders at the center, communications to and from the key-escrow recovery center become a prime target for attack. For instance, some companies had offered an approach where keys were sent to a recovery center using a globally-known public key. The experts concluded: "this is among the worst possible designs from a business point of view: it has a single point of failure (the key of the recovery agent) with which all keys are encrypted. If this key is compromised (or a corrupt version distributed), all the recoverable keys in the system could be compromised."[41]

Along with such risks, the experts emphasized the complexity of building and operating a key escrow system. Complexity is inherently a major challenge in developing and implementing encryption systems. A key recovery system greatly multiplies the complexity, especially given law enforcement and national security desire to access communications within hours or even less. The experts asked readers to consider the complexity of these steps: "reliably identify and authenticate requesting law enforcement agents (there are over 17,000 U.S. domestic law enforcement organizations); reliably authenticate court order or other documentation;

---

[34] Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard" (1994), available at http://www.crypto.com/papers/eesproto.pdf.

[35] One vehicle for the political mobilization of the technology community was Computer Professionals for Social Responsibility, whose program office for Privacy and Civil Liberties became the Electronic Privacy Information Center in 1994. http://cpsr.org/prevsite/program/privacy/privacy.html/.

[36] [cite Trustwrap and 1993 changes]

[37] John Perry Barlow, "Decrypting the Puzzle Palace," Communications of the ACM (July, 1992), available at http://www.scribd.com/doc/1788623/EFF-Surveillance.

[38] Department of Commerce, "Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List," 61 Fed. Reg. 68572, 68573 ("The plan envisions a worldwide key management infrastructure with the use of key escrow and key recovery encryption items."). Key escrow was no longer U.S. government policy after 1999, when the Administration shifted to support of strong encryption.

[39] The paper was drafted and signed by a who's who of encryption experts: Hal Abelson, Ross Anderson, Steven Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter Neumann, Ronald Rivest, Jeffrey Schiller, and Bruce Schneier. The paper was published by the Center for Democracy and Technology as "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption" (May 27, 1997), available at http://www.schneier.com/paper-key-escrow.pdf.

[40] Id. at 11.

[41] Id. 18.

reliably authenticate target user and data; check authorized validity time period; recover session key, plaintext data, or other decryption information; put recovered data in required format; securely transfer recovered data, but only to authorized parties; reliably maintain an audit trail." [42] Each step is subject to possible attacks, such as fake presentation of law enforcement credentials or a court order. Because so many parties interact, it is enormously complex to enable law enforcement access, while rigorously excluding unauthorized access. The third dimension highlighted by the experts is the likely large cost of creating and maintaining such a complex system. Costs include: the overhead of operating the system; product design and testing costs, to assure the highest level of security consistent with key escrow; and costs on all the users who are required by law to comply with key escrow requirements, including costs to users in the form of likely compromised communications. In the face of such a comprehensive critique, any plan to move forward with key escrow should only take place after full consideration of the multiple vulnerabilities and costs inherent in the key escrow approach.

2. Export controls and proposed limits on domestic encryption. After the failure of the Clipper chip, the Administration continued to support the position of the FBI and the NSA, that strict limits should exist on the use of strong encryption through communications networks and more generally. The crypto debates focused primarily on export controls and secondarily on proposals to create limits on domestic use of encryption in the U.S.

For people new to the topic of encryption, it may initially seem odd that encryption products were historically considered "munitions," and thus subject to the sorts of export rules that applied to advanced military technologies such as fighter jets or other advanced weapons.[43] The history of Enigma in World War II, however, illustrates the military importance of breaking enemy codes and ensuring the security of allied communications.

The precise details of the export regime shifted over time, with varying roles for the Commerce, State, and other departments. The regime had two primary parts, licenses and regulations. Export of even moderately strong encryption required a license from the export office in the Department of Commerce. Companies that were pushing the envelope on encryption export faced the risk of denial and inability to sell their goods overseas. The government would also periodically issue regulations that applied more broadly than an individual license. A 1996 regulation, for instance, said: "The plan envisions a worldwide key management infrastructure with the use of key escrow and key recovery encryption items."[44]

The export control regime meant that major information technology companies were constantly in difficult negotiations with the federal government about encryption, especially because products were evolving so rapidly during this period of intense Internet growth. Export limits placed burdens on the many IT companies that had substantial sales overseas. Those companies faced difficult choices about how much to sell products everywhere that had known weak encryption, or else to have two tiers of products, one for use in the United States and one exported abroad. The export rules over time also faced mounting criticism for their effect on U.S. sales; strong encryption products that were created outside of the United States were not subject to U.S.

---

[42] Id. at 15.
[43] See OFFICE OF TECHNOLOGY ASSESSMENT, CONGRESS OF THE UNITED STATES, INFORMATION SECURITY AND PRIVACY NETWORKS 115, OTA-TCT-606 (1994) at 121.
[44] Department of Commerce, Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68572, 68573 (Dec. 30, 1996).

export control rules. A growing concern was thus that strong encryption was in fact being deployed outside of the U.S., but the export rules were preventing U.S. companies from meeting that demand.

The stakes became even higher in 1997, when the House Intelligence Committee passed a bill, drafted in large part by the FBI, which would have imposed criminal penalties on the manufacturing or distribution of domestic encryption products that did not contain a government-mandated back door. Previously, the U.S. had permitted research and use of strong encryption within the country. Limiting the strength of domestic encryption was a logical component of the FBI view that it should have the ability to decrypt communications that it lawfully received, including for U.S. communications. Limits on domestic encryption also were important to the FBI because of doubts about the effectiveness of export controls – software widely deployed in the U.S. over time would likely spread globally, despite export rules. Proposed limits on domestic encryption, however, shifted the intensity of the crypto wars to a new level, directly affecting many users and researchers who were not involved in the export of commercial products.

A group of Internet law professors issued a detailed critique of domestic encryption limits that was analogous to the technical critique of key escrow discussed above.[45] The critique first focused on the unprecedented intrusion on free speech from a mandate to give the encryption keys to the government.[46] The proposal created unconstitutional searches under the Fourth Amendment, which generally forbids secret searches by government.[47] The letter also highlighted three policy concerns. First foreign government access to keys meant that Americans' communications would be subject to being read overseas, without the court orders and other legal protections that apply in the U.S. Second the United States would "become the leader in establishing a global surveillance society."[48] Key escrow created threats to non-government groups of all kinds, including churches and the press. Third, a global key escrow regime would be a threat to U.S. economic security, as the keys of U.S. companies would be subject to misuse in other countries, without notice to the companies, to the advantage of their local competitors.

As the crypto wars continued, the proposal to limit domestic encryption was blocked in Congress. Free speech objections to encryption limits met with some success in federal court.[49] Meanwhile, a form of strong public-key encryption became publicly available. As this PGP (pretty good privacy) software spread, the agency attempts to prevent use of strong encryption became increasingly futile. Once PGP could be easily

---

[45] The law professor critique was sent as an open letter to the House Commerce Committee. It was drafted by Michael Froomkin, Lawrence Lessig, and Peter Swire, and was published by the signed by an additional 25 law professors, and published by the Center for Democracy and Technology. Available at http://www.interesting-people.org/archives/interesting-people/199709/msg00054.html.

[46] Id. ("This amendment regulates citizens before any finding of probable cause. It regulates the programs that citizens may use before they speak at all. It requires every citizen to fit his speech to a program essentially designed by the government, so that the government is better able to monitor the citizen's speech.").

[47] Id. ("By requiring users of encryption to place their key with third parties who can be compelled under the statute to hand that key over to the government, the amendment makes possible secret searches by the government on an unprecedented scale.")

[48] Id.

[49] Bernstein v. U.S. Department of Justice, 945 F. Supp. 1279 (N.D. Cal. 1996). The case involved college professor Daniel Bernstein who wished to publish an encryption algorithm, but the export control rules required him to obtain an export license before publication. The court held this prior restraint on publication violated his free speech rights under the First Amendment.

downloaded from anywhere in the world, members of Congress and others increasingly realized that the controls should be lifted. A large and growing portion of the Congress signed letters supporting legislation that would lift the encryption export controls.[50]

3. The 1999 shift in administration position. In September, 1999, the Clinton administration shifted position and announced that it would lift most export controls on encryption. Secretary of Commerce Daley said: "These regulatory changes basically open the entire commercial sector as a market for strong U.S. encryption products. Exports to governments can be approved under a license."[51] The White House announced that "[a]ny encryption commodity or software of any key length can now be exported … without a license … after a technical review, to commercial firms and other non-government end users in any country except for the seven state supporters of terrorism."[52] The administration explicitly endorsed the view that strong encryption is needed on the Internet. Peter Swire, the administration's Chief Counselor for Privacy, said: "[T]oday's announcement reflects the Clinton administration's full support for the use of encryption and other new technologies to provide privacy and security to law-abiding citizens in the digital age…. Especially for open networks such as the Internet, encryption is needed to make sure that the intended recipients can read a message, but that hackers and other third parties cannot."[53]

The 1999 announcement decisively changed U.S. law and policy on encryption and brought the crypto wars effectively to an end. Determining the key factors in the shift is subject to debate. Politics certainly played a part, including effective advocacy by the IT companies and privacy advocates and Vice President Gore's desire to have their support heading into the 2000 presidential election.[54] Members of both parties in Congress were increasingly opposed to the old administration position, based significantly on the view that American companies would otherwise lose market share and strong encryption would be widely available anyways from other countries.

My view is that the merits of the case were extremely important to the eventual shift in position. Any government is inclined to listen closely to law enforcement and national security advisors when they warn of a problem caused by a new technology such as encryption. Over time, though, two basic conclusions became clear to almost everyone involved: (1) strong encryption is essential for an open network such as the Internet to succeed; and (2) no technical fix, such as key escrow, is workable to give only the "good guys" access to those

---

[50] [cite to number of Senators and Representatives who signed petitions supporting the SAFE Act.]

[51] The White House, Press Briefing by Deputy National Security Advisor Jim Steinberg, Attorney General Janet Reno, Deputy Secretary of Defense John Hamre, Under Secretary of Commerce Bill Reinsch, and Chief Counselor for Privacy at OMB Peter Swire, Sept. 16, 1999 (Statement of William Daley); available at http://intellit.muskingum.edu/cryptography_folder/encryption2.htm. [hereinafter "Press Briefing"].

[52] White House, Statement of the Press Secretary, "Administration Announces New Approach to Encryption," Sept. 16, 1999. Available at http://www.techlawjournal.com/cong106/encrypt/19990916wh.htm.

[53] Press Briefing, *supra* note __ (statement of Peter Swire).

[54] A tricky task in Washington is when to be cynical about public policy but not too cynical. Shortly after the White House announcement, Swire was asked by a reporter whether the timing of the announcement was synchronized with a fund-raising trip that week to Silicon Valley by the Vice President. Such conspiracy theories are often wrong. Having lived through the process from the inside, Swire assured the reporter that the timing instead depended on much more banal factors, such as when the much-negotiated final language was cleared by all the agencies, and finding a day with the Attorney General, Secretary of Commerce, and other officials could all attend.

encrypted communications and not the "bad guys." In the White House announcement, Deputy Secretary of Defense Hamre echoed these points: "We in the Defense Department did it [i.e., supported the new policy] because I think we feel the problem more intensely than does anyone else in the United States. We are the largest single entity that operates in cyberspace. No one is as large as we are. We are just as vulnerable in cyberspace as is anybody, and we strongly need the sorts of protections that come with strong encryption."[55]

B. Encryption Issues Today in India, China, and Globally

Encryption policy developments in India and China are noteworthy not only because of their relative size and power, but also because they represent divergent approaches to today's information reality. Whereas India currently supports a weak encryption system in the interest of national security, China has sought to encourage domestically produced encryption products.

The outcome of encryption policy debates in India and China will have enormous implications for the nature of the global Internet and telecommunications infrastructure. If weak encryption becomes the norm for these major markets and populations, then the cybersecurity of the Internet more generally will be importantly weakened. While each nation has its internal dynamics for resolving encryption issues, many of the current concerns were expressed and debated during the crypto wars of the 1990's. Accordingly, it is important keep in mind the lessons learned in the 1990's when examining the emerging encryption debates, in India, China, and elsewhere globally.

1. India. [This section will get more detailed citations for step-by-step history and legal rules.] India's current encryption policy can best be understood as a response to the 2008 Mumbai bombings, which left 200 dead and over 700 injured. Responsibility for the attacks was widely attributed to Pakistani funded terrorist groups. In the aftermath of the attacks, the Government of India and national security agencies have launched an ambitious plan to increase their lawful intercept capabilities and to ensure that encryption will not block access to communications. In 2010, a highly publicized dispute with Research in Motion (RIM), the manufacturer of Blackberry, centered on India's demand for the keys to encrypted message transmitted over the Blackberry Enterprise Server. Creation of a uniform national encryption policy has thus become an important issue in New Delhi.

The Indian Telegraph Act of 1885 regulates the use of telegraphy, phones and other forms of communication.[56] Under Section 4 of the Act, all telecommunication providers offering wired or wireless services to the public must obtain a license from the government.[57] The licensing regime of the Department of

[55] Press briefing, *supra* note __. (Statement of John Hamre) In Swire's view, the changing position over time of the Department of Defense was important to the administration's eventual decision to shift position on encryption. The NSA is part of the DoD, and its interest in reading communications was predominant at first, leading to the Department's support for limits on encryption. Over time, however, DoD increasingly realized its own dependence on the Internet and thus on effective encryption. In addition, DoD wished to retain world-class encryption skills within the United States, and did not want strong encryption to be provided primarily from the rest of the world. Once the DoD recognized these arguments in favor of effective encryption, the FBI and Department of Justice were increasingly isolated in the inter-agency debates, leading to the 1999 administration decision to shift position.

[56]

[57]

Telecommunications, developed in the late 1990's, prohibits deployment of "bulk encryption", i.e., end-to-end encryption, for international and national long distance service providers, as well as Internet service providers. . It also restricts end users from using encryption, or systems (e.g. Blackberry) providing encryption, with greater than a 40-bit key length.[58] Up until the 2008 Mumbai bombings, these rules were not widely enforced. Indian individuals and corporations regularly use a wide range of encryption telecommunication products and services that employ longer key lengths, including: SSL (for E-commerce); HTTPS (for secure web browsing); virtual private networks; voice communications such as Skype; and mobile e-mail communications such as those provided by RIM Blackberry.

Meanwhile, different encryption standards exist for other government agencies. For example, financial agencies are permitted to use stronger encryption than other agencies. The Securities and Exchange Board has issued Guidelines on Internet Based Trading and Services, which permit up to 128-bit keys, and Internet banking guidelines for the Reserve Bank of India requires at least 128-bit SSL. These varying standards have prompted calls for a modern and uniform national encryption system. Section 84(a) of the Information Technology Act of 2008 permits the government to develop a new encryption policy, which would fall under the Information Technology Act, independent of telecom licensing guidelines.

Conflicts between India's national security policy and international commercial practice have led to public disputes with RIM, Google, Skype, and other communications companies. The national security agencies seek real-time access to intercepted, encrypted communications. Section 69 of Information Technology Act of 2000 provides that the government can intercept, monitor or decrypt any electronic data for national security purposes.[59] The government can order the lawful interception of communications under the authority of Section 5(2) of the Indian Telegraph Act of 1885 with a written order.

RIM and other providers have repeatedly stated that they do not have the ability to turn over the decryption keys to the government because only the end users possess them. RIM's position is consistent with the authors' own understanding of how the Blackberry Enterprise System operates.[60] In response, the government has threatened to shut down providers who do not comply with the strict legal limits on encryption, including the 40-bit limit on key length.

Based on interviews conducted in India and elsewhere by one of the authors (Swire) in 2011, the current controversy in India is similar to the U.S. crypto wars of the 1990s. Indian national security and law enforcement agencies are encountering technical obstacles to their wiretaps, including the use of encryption. These agencies are seeking to reinforce the existing legal rules, so that new technologies will be easier to wiretap. One category of opposition comes from technical experts (both inside and outside of the government) and the information technology industry, which emphasize how effective encryption and related technologies are essential to modern computing. Another category of opposition comes from domestic Indian industry, especially the BPO (business process outsourcing) industry. The BPO sector risks losing business to competing countries if consumers cannot trust that their data will be well protected when transferred to India.

In 2011, interviews with officials indicated serious consideration of a key escrow solution for India, reminiscent of the Clipper Chip proposal in the U.S. As was true in the United States, key escrows initially

[58] Section 32.1 licensing agreement, available at http://www.indentvoice.com/other/ISPLicense.pdf
[59] [cite]
[60] A basic overview of the BES system is available at __

seems attractive because it could simultaneously permit strong encryption for ordinary communications but lawful access in the small subset of cases where there is a lawful intercept. Other parts of this paper explain in detail the severe technical and policy objections to a key escrow approach.

Indian policy for encryption is difficult to predict. The national security argument is treated very seriously in India, which has ongoing tension with its nuclear-armed neighbor, Pakistan. There has been some discussion of imposing import controls on encryption, so that importers would need to obtain licenses in order to bring encrypted products and services into the country. Meanwhile, as discussed in this paper, there are severe cybersecurity, business, and other objections to the limits on effective encryption that India has in current law and is considering expanding.

2. China [additional citations and details to come, especially about China's non-standard algorithms] China's "Indigenous Innovation" policies reflect the government's desire to launch the country into the forefront of the global technology market.[61] In 2006, China revealed its "National Medium and Long-Term Plan for the Development of Science and Technology (2006-2020)," which states, "despite the size of our economy, our country is not an economic power, primarily because of weak innovative capacity."[62] Part of China's push for indigenous innovation involves gaining expertise in the area of cyber security and encryption. China has placed limits on global-standard encryption both through strict licensing regimes and by requiring use of domestic encryption algorithms, which have not been publicly peer reviewed.

a. China's licensing requirements. China's approach to gaining traction in the global encryption market has differed greatly from international standards of open, peer review for encryption standards. China treats encryption as a national policy, under the authority of the government, instead of encouraging growth through private sector development. In 1999 the Commercial Encryption Regulations restricted import and domestic use of encryption to that licensed by China's State Encryption Management Bureau (SEMB).[63] The regulations also prohibited the sale of encryption products produced by foreign countries without a permit and required all providers of encryption products to disclose their source code to the government.[64] Foreign companies balked at the broad scope of the regulation. In response, SEMB issued a clarification in 2000, stating that the regulations would only apply to special purpose hardware and software products whose "core function" was encryption.[65] Examples of "core function" products include personal computing systems and mobile phones.[66] However, China did not specify standards or provide further guidance for determining whether a device has encryption as its core function. This lack of guidance has created great uncertainty among companies wishing to do business in China for any of the wide array of hardware, software, or services that deploys encryption. In 2008, two SEMB Notices suggested that the core/non-core distinction would be abandoned in favor of regulating all commercial encryption products that use encryption for security purposes; however, the distinction still exists for purposes of obtaining an import permit.[67]

---

[61] [cite Indigenous Innovation Policy (to increase domestic innovation and replace foreign IP with domestic IP where possible)]

[62] Preamble of The National Medium and Long-Term Plan for the Development of Science and Technology (2006 – 2020), by the State Council, available at __.

[63] Commercial Encryption Regulations,1999.

[64] Commercial Encryption Regulations, 1999, get pin cite.

[65] SEMC 2000 Notice clarifying the scope of the Commercial Encryption Regulations.

[66] Id, find page.

[67] 2008 SEMB notices and import permit language.

Along with the "core function" rules, in 2007 China required domestic certification for certain product categories. This certification has to be obtained from China's Office of Security Commercial Code Administration before the products can be used, produced and marketed in China. However, the certification process involves disclosure of the products' encryption source code, among other trade secrets, and appears to require the products to incorporate Chinese homegrown encryption algorithms. In the face of opposition from multiple countries and technology industry alliances, China limited the certification requirements to products eligible for government procurement. Due to the large state sector in China, however, government procurement affects a wide range of commercial activities. Implementation of the certification requirements has been delayed twice [68]

Similar to the commercial encryption certification program, in June 2007 China established guidelines in line with its indigenous innovation policy, regulating products integrated into critical infrastructure information systems. This Multi-Level Protection scheme specifies five categories of security, detailing technical standards for encryption products used at each level.[69] Again, these products are required to disclose encryption code [***"code"?] information, among other trade secrets. If the products are above certain levels of security, only Chinese providers can source those products.

b. Homegrown Encryption. As a part of its indigenous innovation policy, China employs a strategy of developing closed, national standards for encryption, which it does not make public. One prominent example is China's trusted computing module (TCM), a chip used to secure data in computers. This effectively shuts the global trusted platform module (TPM) standard out of China's domestic market. [Insert more on TCM controversy]

Another example is China's wireless networking standard, the Wireless Authentication and Privacy Infrastructure (WAPI). Its purpose was to resolve security holes in Wi-Fi (802.11), the global standard for wireless networking; instead, WAPI itself was technically flawed.[70] Foreign wireless companies operating or manufacturing in China were required to partner with one of 11 Chinese companies that possessed the WAPI encryption standard, since the standard was not released to the public. [Insert more on WAPI controversy]

3. Encryption in the rest of the world. [Insert brief discussion of encryption developments in Russia, Brazil, and elsewhere. The main point is that communications over the Internet will increasingly be defined by rules applying in these countries outside of the U.S. and Europe. Good policy, supporting strong encryption, is thus increasingly important on a global basis.]

III. Why Globalization Strengthens the Case for Strong Encryption

The crypto wars of the 1990's led to publication of numerous reasons why strong encryption should be widely used, especially over an insecure channel such as the Internet. This Part examines how the passage of

[68] Written Comments to the U.S. Government Interagency Trade Policy Staff Committee In Response to Federal Register Notice Regarding China's Compliance with its Accession Commitments to the World Trade Organization (WTO), p 17-18, September 27, 2010

[69] [MLP and encryption requirement pin cite]

[70] *http://news.cnet.com/China-battles-rejection-of-Wi-Fi-encryption-algorithm/2100-7351_3-6077975.html*

time and the continued process of globalization further strengthen the case for strong encryption. The first major reason concerns the central role of encryption today in cybersecurity. Encryption is now deeply integrated into the routine functioning of modern computing, far more than was true when U.S. policy shifted in 1999. In cybersecurity today, attackers currently have major advantages over defenders. Encryption is quite possibly the single most important advantage for defenders, and is thus vital to overall cybersecurity. The second major reason is what we call "the least trusted country problem." If there are back doors or limits on effective encryption, then the security of the global system is only as good as the security in the least trusted country. Use of strong encryption is a uniquely effective mechanism for addressing this lack of trust.

A. The Central Role of Encryption in Cybersecurity

As cybersecurity has risen in importance, so too has the need for strong encryption.

1. The surprisingly recent rise of the cybersecurity issue. The importance and difficulty of cybersecurity has become a consensus issue. In the United States, the need to improve cybersecurity is often voiced by both political parties,[71] both the President and the Congress,[72] and both military and civilian agencies.[73] Similar consensus exists in other countries. For instance, speeches by government leaders in India about cybersecurity sound quite similar to American pronouncements.[74]

Although cybersecurity is a consensus issue in 2011, its emergence has been more recent than many would guess. One of the authors has previously written about the strikingly low amount of discussion about cybersecurity issues, other than encryption, in policy discussions through the late 1990's.[75] Discussions at that time about key Internet legal and policy issues mentioned many other topics but omitted cybersecurity. For the U.S. government, the cybersecurity issue received growing attention in preparation for the Y2K problem[76] and in response to denial of service attacks on several major websites in early 2000.[77] In industry, a common pattern during the early years of the commercial Internet was to introduce new products and features as rapidly as possible, with security coming later if at all. One sign of a change was when Microsoft in 2002 stopped all development on its Windows operating system to give engineers ten weeks of intensive security training.[78] Microsoft Chairman Bill Gates wrote to all employees: "In the past, we've made our software and services more compelling for users by adding new features and functionality. . . . We've done a terrific job at that, but all those

---

[71] [cite to Lieberman/Collins quotes]
[72] [cite administration cybersecurity package and announcement of House R committee on cybersecurity]
[73] [cite to Pentagon cyberwar announcement summer 2011 and Commerce Department White Paper 2011]
[74] [cite to 2011 Indian official statements]
[75] Peter P. Swire, "Elephants and Mice Revisited: Law and Choice of Law on the Internet," 153 U. Penn. L. Rev. 1975 (2005), at fn 4.
[76] [define Y2K]
[77] "The federal government got its defining wakeup call about vulnerabilities facing the nation's IT systems in the years and months leading up to Jan. 1, 2000." Timeline: The U.S. Government and Cybersecurity, Washington Post, May 16, 2003, available at http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A50606-2002Jun26&notFound=true. The importance of the denial of service attacks in early 2000 is suggested by an Internet security "summit" that President Clinton held in their wake. [cite]
[78] "Gates seeks to plug security holes," The Guardian, Feb. 13, 2002, available at http://www.guardian.co.uk/technology/2002/feb/13/microsoft.business.

great features won't matter unless customers trust our software. So now, when we face a choice between adding features and resolving security issues, we need to choose security."[79]

This recent rise in attention to cybersecurity is relevant to encryption debates today. In the late 1990's there was no general awareness of the challenges of cybersecurity. Today, cybersecurity by consensus is an important and difficult challenge. This paper explains why encryption is vital to cybersecurity. As a consequence, encryption is vital to an important and difficult challenge facing nations around the world.

2. Cybersecurity and the increasing importance of computing and the Internet. A major reason why cybersecurity is more important today is that computing and the Internet are more important. This conclusion is likely intuitive to most readers, so the discussion here is brief. The rise in E-commerce illustrates this growth. In a 1998 book, the best available estimates of E-Commerce were still less than $1 billion per year.[80] In 2010, online retail sales were over $172 billion and were estimated to continue growing at a ten percent compound annual growth rate through 2014, or over $250 billion.[81] The range of important activities conducted online has similarly multiplied, for personal, business, and governmental organizations.

Globalization expands the range of nations in which the Internet and computing play an important role in society. In 1997 India had fewer than W Internet users and China fewer than X. Today, even a conservative estimate shows that India has over Y people connected to the Internet and China has Z. The fraction of Internet sites hosted in the U.S. has similarly fallen from X percent in 1997 to Y percent in 2010. The proliferation of countries with substantial Internet activity is accompanied by more intensive cross border transfers of information. For example, India's business process outsourcing (BPO) sector has grown exponentially, increasing from $X to $Y in the last decade. This back-office sector now accounts for X% of India's total exports. The twin phenomena of greater internet use and increased trans-border activity means that actions taken by non U.S countries have greater effects on U.S. businesses and organizations and are more important to the function of the Internet itself.

3. Encryption is deeply integrated into modern computing.

[This section will briefly describe major current technologies that use encryption, such as: SSL (E-commerce); HTTPS; VPNs (using both encryption for authentication and encryption between the user and the server); encryption at rest (now standard on personal computers); from wireless phone to tower; etc. The point of this section is to show how deeply encryption is integrated into modern computing. Commenters are welcome to send additional examples or citations to the widespread and important use of encryption today.]

4. The offense is ahead of the defense, making encryption irreplaceable for cybersecurity. A fundamental problem with cybersecurity today is that the offense is ahead of the defense.[82] "Offense" refers to the hackers who wish to penetrate and disrupt or exploit a cyber system. "Defense" refers the owners and users

[79] Bill Gates, "Trustworthy Computing," Jan. 15, 2002, available at http://www.wired.com/techbiz/media/news/2002/01/49826.
[80] Peter P. Swire & Robert E. Litan, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive (1998) [add page cite].
[81] http://techcrunch.com/2010/03/08/forrester-forecast-online-retail-sales-will-grow-to-250-billion-by-2014/
[82] [Add quotations/cites that the offense is ahead of the defense.]

who wish to protect their cyber systems from intrusion. In this era of generally weak defense, encryption is a preeminent defensive tool.

One of the authors has written previously about how cyberattacks differ from attacks in the physical world.[83] First, attacks from a distance are much more common online. In the physical world, a thief has to enter an actual building in order to steal goods. By contrast, in cyberspace, hackers have the ability to launch an attack from anywhere in the world, without risk of physical injury or capture. When defending a physical location, one only has to protect against intruders from your "neighborhood." The global nature of the Internet, however, means that everyone is your neighbor, including distinctly insidious neighbors, such as cyber criminals or hostile nation states.[84]

Second, cyber attacks are cheap while defense is costly. Hacking technology is widely available and attacks can be launched remotely, so the offense incurs only nominal expense. Meanwhile, the defense is only as strong as its weakest point.[85] Because attacks can be launched from anywhere on the web, defenders of computer systems have to expend valuable resources in hopes of having good security at every point. The defense has to be strong everywhere, while the offense only needs to succeed in one place. Third, cyber attacks can be launched repeatedly. A burglar often has to wait for the right moment to try to enter a house. But a remote hacker can look for vulnerabilities 24 hours a day, and use automated attacks to probe for weaknesses repeatedly. Fourth, the source of attack is difficult to determine. The apparent source of attack is often not the actual source.[86] The ability to disguise the source of an attack greatly weakens deterrence, because the defense often has no workable way to locate and punish the attacker.[87] Fifth, size matters less than in traditional physical-world attacks -- an individual or small group of hackers has the potential to inflict damage disproportionate to their relative number or resources. When innumerable attractive targets exist, offenders can concentrate their attack efforts, but defenders are spread thin.

In the face of such formidable challenges, defenders need any cybersecurity advantages that they can get. Encryption is quite possibly the single most important security tool for defenders. It applies to major categories of vulnerability -- data in motion, data at rest, and authentication. With data in motion, encryption is a powerful tool for protecting communications against attacks from all sources. The protected data can be both

---

[83] The principal paper is Peter P. Swire, "A Model for When Disclosure Helps Security: What is Different About Computer and Network Security," 3 J. Telecomm. & High Technology L. 13 (2004). Related issues are addressed in Peter P. Swire, "A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary software, and Government Systems," 42 Houston L. Rev. 1333 (2006).

[84] [Cite Nimrod Kozlovski]

[85] A cryptography textbook says: "Print the following sentence in very large font and paste it along the top of your monitor. **A security system is only as strong as its weakest link.**" Ferguson et al., *supra* note __, at 5 (emphasis in the original).

[86] For instance, a hacker might route an attack through a university, some other unsecured system, or a "bot" owned by someone else but under the control of the hacker. [cite]

[87] Deterrence famously was an essential feature of the Cold War between the Soviet Union and the United States. Under the theory of mutually assured destruction, any would-be initial attacker knew that its missiles would be traced back to the source and thus that its enemy could accurately identify and act against the initial attacker. [cite on mutual assured destruction] For cyber attacks, however, the initial source of the attack often can mask itself by routing the attack through multiple intermediate Internet locations, and these locations typically do not approve of the attack and so are an inappropriate target for retaliation.

for ordinary citizens and for organizations engaged in sensitive government, banking, medical, or other transactions. Strong encryption prevents attackers from accessing the content of the communication. Similarly, for data at rest, encryption protects files residing inside a person's or organization's computer system. Penetration of the system by an attacker typically does not compromise the encrypted files.[88] In addition, encryption is an essential function of authentication over the Internet. Use of effective encryption is vital to distinguishing authorized from unauthorized remote users. One well-known example of encrypted authentication is the key fob sold by RSA and other providers. These key fobs are widely used by government and businesses to provide secure, remote access to virtual private networks.[89] In a typical implementation, the fob displays a randomly generated access code, which changes often, such as once a minute. The user must log in by entering the current access code displayed on the fob. The string of numbers on the user end must match the string of numbers calculated on the server end during that one-minute window. With this authentication system, any hacker that uses an old key will be blocked from entry.[90]

The usefulness of strong encryption underscores the main problems with prohibiting encryption or deploying weak encryption. For data in motion, figure 3 above illustrates an essential fact about the Internet – that unencrypted communications sent from Alice to Bob are vulnerable to unknown or malicious actors at any one of the intervening nodes. With respect to data at rest, lack of encryption may reveal file contents in their entirety if an attacker gains access to the network. This problem with data at rest has prompted some jurisdictions in the U.S. to pass laws that require or strongly incent the use of encryption on business laptops containing sensitive data.[91] In authentication, lack of encryption allows a hacker to read the password or other identification information used in the authentication process. For instance, sending a credit card number, social security number, or national identification number in unencrypted form potentially allows a hacker to pose as that person for future transactions. The risks associated with sending credit card numbers over the Internet were the driving force for the adoption of SSL, as discussed above.[92]

Cyber security defenders do have some other techniques to protect themselves from attacks. One way to stop remote attacks is to disconnect from the Internet altogether. In fact, some military and other sensitive networks use an "air gap" to separate them from the Internet.[93] Though this separation provides security, it also comes at the high cost of convenience and functionality. Firewalls are another important category of defensive

---

[88] The ability of the attacker to penetrate the system could result in the compromise of then encrypted data if the attacker can learn the encryption keys or gain some other authority within the system to access the encrypted files.

[89] In 2011, RSA suffered a security incident, so that its key fobs were apparently compromised. It appears that the security breach essentially came from a data breach of the key information for each fob, known as the "seeds" for each fob. The cryptosystem was not compromised, but instead the keys were revealed and new keys had to be issued. [cite] It appears that this was an embarrassing incident of data breach by a prominent security company, but the underlying technology remains secure.

[90] For an explanation on how cryptology is used in the RSA Fob system, see __ Available at http://www.rsa.com/node.aspx?id=1158.

[91] Massachusetts law sets strict penalties for loss of a laptop or other loss of data unless strong encryption is in place. [cite] A number of state data breach laws do not require notice in the event of a data breach of the data was effectively encrypted. [cite].

[92] *See supra* text accompanying notes __(describing SSL).

[93] definition on Air gap

tools.[94] Firewalls are used to protect networks from unauthorized access while permitting legitimate communications to enter. Such firewalls are essential to protecting an organization's systems from certain outside attacks. The do not, however, protect data in transit through the Internet, or protect data stored within a system from an intruder. Nor do they provide a tool for authenticating users remotely. These other tools are most effective when used in conjunction with strong encryption.

In conclusion, strong encryption has become a pervasive and preeminent part of cybersecurity. For data in transit, data at rest, and authentication, there is no effective substitute for strong encryption. Any legal regime that prohibits the use of strong encryption thus pervasively undermines its cybersecurity.

B. Globalization and the "Least Trusted Country" Problem.

What we call the "least trusted country" problem is another example of how Internet security is only as strong as the weakest link. If one country prohibits effective encryption, then communications that comply with that country's laws will be compromised. If Alice is in that country, or uses weak encryption as required by that country, then the Bobs of the world will have their communications compromised as well.

Key escrow provides a vivid example of the least trusted country problem. Based on interviews by one of the authors in India in 2011, the government there has been seriously discussing requiring key escrow. Suppose that India carried through on this approach, and that other countries followed suit. The least trusted country problem is a thought experiment – how would Indians feel if Pakistan had the keys as well? In that case, sensitive communications by Indians would be exposed to a country that it has fought wars against in the not-too-distant past. The same logic applies to whatever country a person trusts least. Other examples of distrust might include China and Taiwan, Israel and Iran, and so on.

The least trusted country problem extends beyond key escrow to other limits on effective encryption. Current law in India limits encryption to a 40-bit key, so short that is was trivial to break with inexpensive equipment over a decade ago.[95] For most of the dozen years that India has had that law, there was no visible enforcement and individuals and companies routinely used stronger encryption. That changed, however, after the 2006 Mumbai bombings. Indian security agencies became more concerned about compliance with existing law. In 2010, when India sought keys to read communications through Blackberries, the encryption problem hit front pages in the U.S. and around the world.[96]

Regular enforcement of the 40-bit limit in India would weaken the Internet globally. The BPO sector in India illustrates the problem. Indian back-office services routinely transmit health, financial, and other sensitive information to the United States, Europe, and elsewhere.[97] In the absence of strong encryption, the prudent assumption is that that data will be easily compromised. With a large Indian industry that processes sensitive data, and a national population of well over a billion people, a large volume of Internet and other communications will be insecure.

---

[94] [cite]
[95] *See supra* note __ (describing low cost and short time needed to break a 40-bit key in 1996).
[96] [cite front page story in WSJ]
[97] [cite on countries that use India for back-office services, by sector]

A similar analysis applies to insistence on unproven algorithms in China, which has its own large population and heavy Internet use. Experienced cryptographers have learned not to trust a cryptosystem until it has undergone rigorous and repeated testing in peer review process. Unproven algorithms also have a far higher risk of containing back doors. Internet communications that originate or end in China and use the algorithms should thus be presumed compromised. If unproven algorithms are required for hardware production, such as for computer chips, then devices using those chips should also be presumed insecure. Creating even more risk, vendors who wish to do business in China might incorporate the unproven algorithms into products and services used outside of the country. In this way, one nation's use of weak encryption can undermine security on the Internet more generally.

Laws that limit effective encryption create security holes. Communications that originate, end, travel through, or comply with the policies of those nations are systematically less secure. They are as secure as they would be in the hands of our least trusted country, whatever country that may be.

This analysis shows how globalization increases the importance of strong encryption. In the 1990's, there was indeed some discussion about whether the United States would help create key escrow regimes in other countries.[98] The dominant focus of debate, however, was on how key escrow would operate within the United States. The question was how much to trust independent key recovery organizations in the United States, with its history of civil liberties and the rule of law. Even in that setting, the policy arguments against key escrow turned out to be persuasive.

The arguments against key escrow, or other limits on effective encryption, are even more persuasive in a world with several, or 20, or 200 countries that may impose such limits. If keys are held in numerous countries, then there are many routes to compromise. A key recovery organization may provide the keys even in the absence of court orders or other rule-of-law protections. A supposedly independent organization might be coerced to turn over the keys to the local government. Criminals or others might corrupt insiders at the organization, putting the keys in the hands of malicious parties.

Think about important communications in the hands of the country you trust least in the world. That is the Internet that limits on strong encryption would create.

IV. Responses to Common Concerns

This Part will address commonly expressed concerns about the widespread use of strong encryption, including: (1) the view that backdoors to strong encryption systems exist; (2) the concern that law enforcement and national security agencies will "go dark" if unfettered use of strong encryption is permitted, and (3) the goal of some countries to use encryption regulation as a tool for international trade advantage. In response, this Part will argue that: (1) there are important reasons to doubt the prevalence of backdoors; (2) surveillance today should be understood as a "golden age of surveillance" rather than a period of "going dark," and (3) trade considerations should not impede the use of strong encryption.

A. Backdoors are Unlikely in Cryptosystems, but More Likely Elsewhere

[98] [pinpoint cite to CDT technical paper, about international ramifications of key escrow]

As discussed above, a "backdoor" provides a software or hardware creator with access to the contents of a communication or file without the permission or knowledge of the user. A backdoor can be simply understood as a security flaw in the design of a system. This flaw may be used to expose the system to law enforcement agencies through lawful process, as was proposed with the Clipper Chip, or the flaw might be designed by software or service providers who use the backdoor for secret access themselves. In interviews with Indian government officials, a commonly voiced concern is that surveillance agencies in the U.S. or other countries are granted access into allegedly strong encryption systems via backdoors but that other nations are denied similar access. If true, the existence of such backdoors would serve as a reasonable rationale for imposing limits on the use of strong encryption in those nations that lack backdoors. Otherwise, allowing unfettered access only to the United States or a few chosen allies would be unfair and a national security risk for India and other countries that lacked such access.

1. Backdoors and Cryptosystems. [With apologies to the readers, the discussion on backdoors needs a thorough organizational and stylistic edit.] Backdoors are inherently insecure. A backdoor is supposed to enable access for those who know the secret (the "good guys"), but deny access to all others (the "bad guys"). For encryption, however, the number and range of others is large. Attackers, for instance, can include Ph.D. computer security experts who benefit professionally from exposing security weaknesses. Along with academic experts, there are "white hat" hackers who make a living by detecting software flaws and informing the authors or the public about bugs in the system.[99] Other potential attackers include criminals, including large organized crime operations that have the resources to hire costly computer security talent.[100] Other potential attackers include foreign governments or entities controlled by foreign government intelligence services. In addition, creators of backdoors have to worry about insider attacks – the possibility that someone on the team that created the backdoor will disclose the secret.

To illustrate this point, consider the Wikileaks disclosures. The leak of hundreds of thousands of U.S. government classified messages in 2011 exemplifies the difficulty of keeping secrets in the Internet age.[101] In reference to whether backdoors exist for encryption systems, what is the likelihood that the highly intelligent academic computer security experts PhDs and white hat hackers have not found any existing backdoors in strong encryption systems since the 1999 U.S. approval of strong encryption for export?[102] Also, assume an internationally recognized company such as Microsoft develops an encryption product with a secret backdoor through which law enforcement can access user data transmissions and communications. If the backdoor were discovered, the company would incur severe enforcement penalties across the world, in addition to the irreparable damage to its brand, loss of consumer trust, and drop in market sharing. These potential repercussions provide businesses with a huge incentive not to install backdoors in their products.

---

[99] See Jennifer Stisa Granick, The Price of Restricting Vulnerability Publications, 9 INT'L J. COMM. L. & POL'Y 10 (2005). One method of uncovering software flaws is through information sharing systems such as the Computer Emergency Response Team operated by Carnegie Mellon University and other similar information sharing systems. For more information, see www.cert.org

[100] Organized crime FN and role in computer hacking

[101] Wikileaks info

[102] Basic encryption systems such as RSA and AES were developed well before 1999 in 198X and 199Y respectively. If white hat attackers had discovered flaws in the algorithms there is every reason to believe these discoveries would have been made public, if only when some remedy for the flaw was deployed. The likelihood of an intentionally designed flaw by major software companies is even lower. For instance, Microsoft deploys the crypto software BitLocker in its Windows software. FN – to BL and how it operates on Microsoft website

It is a very difficult challenge to ensure open access and knowledge of the backdoor to legitimate actors while denying access and knowledge of the backdoor to all others. One of the authors of this article has previously written about the role of secrecy in computer security. This research highlights the fact that such secrecy is unlikely to succeed in the face of so many different attackers with the ability to launch multiple attacks, and report about these successful attacks.[103]

Generally, physical backdoors are easier to implement and maintain than software backdoors. In this situation, attackers expose themselves to significant risk when approaching a target. Each attack is a major undertaking and physical capture of the attacker can end communication with other attackers on the inside of the system. There are thus strong theoretical reasons to believe that backdoors are unlikely remain undetected for computer security than for physical security.

This analysis illustrates the difficulty of maintaining a secret backdoor in encryption systems and other widely used software that is subject to public scrutiny. Computer security experts are familiar with the phrase "no security through obscurity," referring to the concept that an encryption system developed in a closed, secret environment is not trustworthy.[104] If a system is in fact made available to the public and subjected to rigorous peer review, any existing backdoors will likely be discovered.

Law enforcement and intelligence agencies can still retain an advantage in the interception of data without compromising strong encryption systems. One such method is for these entities to intercept data before it is encrypted. For example, an intelligence agency might access Alice's system with a keystroke logger or camera that reveals her keystrokes before she sends the message to Bob.[105] Similarly, the agency might access Bob's hard drive once the message is received through the installation of a rootkit, or with the cooperation of Bob's employer.[106] Another method would be to exploit any gaps in the encryption system. Some wireless telephone companies offer encryption from the sender of the communication to the phone company's switch. An intelligence agency then may access the decrypted communication at the switch before it is re-encrypted and routed to the recipient of the call.[107] These three types of compromise – at the sender, recipient, or at the telephone network – provide law enforcement and national security agencies with an edge without relying on any weakness or flaw in the encryption system. They rely instead on obtaining access to the data at points when it is not encrypted. (*Information or cite to how often these methods are used and how successful they have been?)

Another category of compromise exists at the implementation stage of an encryption system. The hardware or software implementation of a cryptosystem raises subtle security issues, which may not be discovered during the design process. In practice, system architects generally implement encryption algorithms and protocols by drawing on an existing encryption "library." One well-known example is OpenSSL, "a full-

[103] Peter P. Swire, A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems," 42 Houston Law Review 1333 (2006). Also see "A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?" 3 J. Telecomm. & High Technology L. 163 (2004).
[104] No security through obscurity origin
[105] Keystroke logger info
[106] rootkit info
[107] Press reports skype in China

strength general purpose cryptography library" resulting from a "collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer" and other protocols.[108] As an open source library, OpenSSL is used globally, including with the substantial fraction of web servers that use Apatche software.[109] OpenSSL has been widely deployed and subjected to vigorous testing for many years, during which numerous security flaws and bugs have been remedied by software updates.[110] This illustrates the difficulty in establishing watertight security even when deploying publically available encryption algorithms. Intelligence agencies, therefore, can potentially discover weaknesses in encryption systems when implemented, even when strong encryption algorithms are used.

2. Greater likelihood of backdoors for encryption systems that have not been publically tested. The discussion about backdoors has thus far only addressed major encryption systems subjected to sustained testing over a long period of time. This sort of peer review is historically essential to the level of trust placed in the encryption system. Open testing of encryption has been a central tenet of the field, at least since the 1883 writings of Auguste Kerckhoff, who argued that "[t]he system must not require secrecy and can be stolen by the enemy without causing trouble."[111] Cryptographers do not tend to think of a cryptosystem as unbreakable; instead they gain confidence in a system as it withstands repeated empirical testing by high-level exports over a considerable amount of time.

This empirical approach to assessing the strength of an encryption system is directly related to the likelihood of a backdoor. When an encryption system undergoes widespread and intense public testing, it is unlikely that a hidden backdoor exists. By contrast, an untested cryptosystem cannot provide the same assurances for its users – i.e. the encryption system is likely to have a range of security flaws, including the possibility of a backdoor undiscovered by testers.

This importance of sustained peer review is a critical reason why international standards favor cryptosystems that have been proven to withstand repeated attacks. Today, the Chinese government promotes the use of home grown cryptosystems based on algorithms that have not been subjected to significant peer review.[112] Without such testing, users of these encryption systems cannot rule out the existence of intentional backdoors. This risk makes it perilous for such systems to be deployed commercially. These considerations serve as a principled basis for the finding that homegrown, untested cryptosystems are not consistent with best practices for international standards for strong security. [Readers: we welcome citations or more details on peer review and international encryption standards.]

B. "Going Dark" v. A "Golden Age for Surveillance"

[108] See www.openssl.org for more information.
[109] In January 2011, the Apache HTTP open-source web server had just over 59 percent of the web server market share. Netcraft's January 2011 Web Server Survey, available at http://news.netcraft.com/archives/2011/01/12/january-2011-web-server-survey-4.html.
[110] For more information on security problems fixed in released versions of the Apache HTTP Server see http://httpd.apache.org/security_report.html.
[111] Steve Bellovin, June 2009, "Security through obscurity," Risks Digest, referring to Kerckhoffs' second principle.
[112] For more information on Chinese home grown encryption standards, see:

A repeated concern for law enforcement and national security agencies is that they are "going dark" – new forms of Internet and other communications are taking place in ways that the agencies cannot wiretap and decode. This concern is correct in important respects. In some instances, agencies do lose access to categories of information that they previously relied upon.

The discussion here, however, argues that the concern should not be a basis for imposing limits on strong encryption. The limited losses to agencies are accompanied by numerous and significant new surveillance capabilities. Today should be understood as a "golden age for surveillance," in which surveillance activities are in fact greatly enhanced compared to previous periods. Surprising as it may sound to some, the agencies are actually gaining a great deal from the current mix of technologies. The "going dark" argument should not be the basis for limiting use of strong encryption and reducing the overall security of the global communications system.

1. The "Going Dark" Problem. Law enforcement and national security agencies object to the use of strong encryption in electronic communications for one main reason: the agencies are losing some surveillance capabilities that they previously relied upon. The use of wiretaps and relatively easy access to stored records has historically served as important tools for these agencies. When strong encryption is used to secure emails or mobile phone calls, agencies can access the communications but are unable to decipher their encrypted forms. If agencies gain access to encrypted laptops or other forms of encrypted data at rest, the lawful interception process is similarly frustrated.

In 2011 testimony, FBI General Counsel Valerie Caproni described the problem in this way: "We call this capabilities gap the "Going Dark" problem. 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."[113]

"Going dark" is an evocative and compelling image. The phrase invites us to imagine communications shrouded in darkness – cloaked in encryption – so that the eyes of the agency are blind. Although we may want justice to be "blind," in order to achieve impartiality, we surely do not want our police to be blind.

In the 1990's, the "going dark" argument was often made by the FBI and NSA, although the term itself was not widely used.[114] In 1994, CALEA was enacted to address FBI concerns that the shift from copper wires

[113] House Judiciary Comm., Subcomm. on Crime, Terrorism, and Homeland Security, Feb. 17, 2011 (statement of Valerie Caproni). Caproni used the term specifically concerning CALEA-style problems, saying that "the FBI and other government agencies are facing a potentially widening gap between our legal authority to intercept electronic communications pursuant to court order and our practical ability to actually intercept those communications." As shown by the quote in text, however, the real objection by the agencies is broader, applying to "the gap between authority and capability." This paper thus uses the term "going dark" to refer to the full range of gaps between authrority and capability, notably: (1) CALEA-type problems where lawful process does not get access to a communications; (2) issues of strong encryption for communications, where the agency receives the communication but cannot decrypt it; and (3) issues of strong encryption at rest, where the agency gains access to a laptop or other device, but cannot decrypt it.

[114] The authors are not aware of the term "going dark" systematically being used for these issues until its recent prominent use by the FBI in connection with CALEA issue.

to fiber optics made traditional wiretaps less useful. The NSA's ability to collect communications was threatened during this period as a greater proportion of international calls shifted from radio communications (often easy to intercept by the agency) to fiber optic cables (generally easy to intercept only at a switch controlled by a telecommunications company). Coupled with the rapid development and widespread availability of strong encryption, the agencies faced the likelihood that many communications would not be as readily accessible as before. The Clipper chip was one proposed response to these challenges facing the agencies.

Despite these risks, in 1999 the U.S. government decided to embrace the use of strong encryption. As discussed above, arguments in favor of Internet security, civil liberties, and international trade prevailed over the surveillance agencies' objections. The government ultimately recognized the private sector's need for and dependence on strong encryption, and identified the inherent value in using strong encryption for law enforcement and national security purposes. Despite losing the crypto wars, important agency concerns were addressed. The FBI received enhanced funding for its technical capabilities, and this funding has continued to grow over time.[115] Together, government and industry leaders worked to develop the system of public-private partnership that continues today, in which industry experts meet with the government about encryption and technology for the carrying out of lawful intercepts.[116]

2. Today as a "golden age for surveillance."[117] The Internet and the rapid advancement of IP-based communications do present new obstacles to lawful interception. At the same time, these technological developments also provide law enforcement and national security agencies with powerful new surveillance capabilities. The discussion here highlights three areas where law enforcement has far greater capabilities than ever before in human history: (1) location information; (2) information about contacts and confederates; and (3) an array of new databases that create "digital dossiers" about each individual's life.[118] This information about any individual suspect is made even more useful because of the way that data mining can help identify suspects.

We are entering a new age where most people carry a tracking device, the mobile phone. Location information comes standard with a wireless network – the phone company needs to know where your phone is to send you the call. A specific cell handles the call, so the network knows what cell you are in. Location information is tremendously useful for law enforcement and national security agencies. It can put a suspect at the scene of a crime, or establish an alibi. It can act as a "bug" without the need for the agency to go through the risk and bother of placing a bug on the suspect's person or property.

The precise rules for storing this location data vary by jurisdiction and wireless carrier. In many instances, though, the routine practice is that location data is stored for a significant period of time.[119] Carriers

[115] [cite to promise for FBI funding in 1999 encryption announcement, and statistics on funding level over time]
[116] [cite to information about these partnerships]
[117] The text describes "a" golden age for surveillance rather than "the" golden age for surveillance. As described in Alan Westin's unpublished history of privacy, there have been previous periods of especially effective surveillance, from ancient Sparta to the Nazi regime in Germany. (Document on file with authors.)
[118] Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. Cal. L. Rev. 1083 (2002).
[119] The European Union has had ongoing debates between law enforcement agencies and data protection agencies about data retention for phone calls. [cite] The Data Retention Directive of 2006 requires retention of

in the U.S. are subject to data preservation orders, so that location information on known suspects is retained once a proper agency request has been made.[120] The number of requests from law enforcement for such location information has climbed sharply in recent years, at least according to statistics in the United States.[121]

It is true that the cautious suspect can try to avoid this location tracking, such as by using a prepaid cell phone or not carrying the phone when doing criminal activities. Some countries have placed limits on non-identified mobile phones, however,[122] and the suspect has to worry that his or her confederates will show up at a meeting carrying their regular mobile phone. More generally, a tremendous number of people now carry cell phones as they go through their daily life. Location information thus becomes available for surveillance purposes in ways never before possible in history.

Information about a suspect's or witnesses' confederates is the second category of information newly available in rich detail to the agencies. For many investigations, who is called is at least as important as what is said in the call. The investigator gets leads on whom else to investigate, and can follow those leads to the contact's contacts, and so on.

The importance of confederates has become famous in social networking. The term "social graph" was coined, in connection with Facebook and other social networks, to describe the phenomenon of "the global mapping of everybody and how they're related."[123] For investigatory agencies, mapping everybody and how they are related is extremely, extremely useful. Social networking sites themselves will become an increasingly important source of investigatory material in coming years. The phenomenon is much more general, however:

- A generation ago, long-distance phone calls were expensive, and international calls a rare and costly event in most people's lives. As costs have plummeted, the volume of local, long-distance, and international calls has grown sharply over time.[124] Calling records show the to/from information for calls already made, pen register orders reveal who a person is calling, and trap-and-trace orders show who is calling the person. The number of such orders in the U.S. has climbed sharply over time.[125]
- The explosion of mobile phone use has supplemented the rise in wireline calls, and mobile use continues to increase rapidly. India, for instance, was showing an astonishing 17 million new wirelines per month in 2011.[126]
- E-mails have become a pervasive feature of life for many people. The volume of emails has grown in the past twenty years at more than an x% rate.[127] The emergence of global web mail providers including

---

phone records for six to 24 months. [cite, with reference to location data specifically] In the United States, data retention bills have advanced in the Congress, but have not become law as of 2011. [cite to 2011 bills]

[120] [cite to data preservation requirements]

[121] [cite to number of location request orders in the U.S.]

[122] Purchase of a mobile phone in India, for instance, requires photo identification and registration of the phone with the government. [cite]

[123] Facebook: One Social Graph to Rule Them All? April 21, 2010, available at http://www.cbsnews.com/stories/2010/04/21/tech/main6418458.shtml

[124] [cite on cost/minute and volume of wireline calls]

[125] [cite to annual wiretap orders; cite to number of national security letters in the 2000's, according to the Inspector General Report of DOJ]

[126] [cite to India wireless statistics]

[127] [cite]

Gmail and Hotmail provides investigatory agencies the convenience of serving many lawful requests to a small number of providers.

- Text messages are another source of investigatory material. The rise of unlimited text messaging plans in many jurisdictions provides numerous clues about a person's key confederates, and the time and date of their communications.
- VOIP (voice over Internet Protocol) calls are growing rapidly. Skype was sold to Microsoft for $8.5 billion in 2011. Even for Skype calls whose content is encrypted, Skype connects the callers and so the to/from information is subject to legal process.

These wireline calls, wireless calls, e-mails, texts, VOIP calls, and social networking records are treasure troves of information to investigatory agencies about a person's confederates. In the bygone era of face-to-face communications, no trace was usually left after the fact of whom a suspect had talked with. Today, by contrast, an individual would need to abstain from many everyday activities to prevent the government from obtaining access to records providing information about his or her contacts. The identity of those contacts helps lead investigators to additional targets of interest, thereby painting a broader and more precise picture of potential criminal or national security activity.

Information about location and a person's confederates, in turn, are simply examples of the larger trend towards detailed personal records. Consider the amount stored an individual's personal or work computer. A standard laptop today often holds many gigabytes of data, more than a mainframe computer could hold 20 years ago.[128] If the government obtains access to an individual's personal or work computer, it is highly likely that the computer will reveal detailed and diverse records about the person's life. The records retained on that computer, in turn, are only a small subset of the records stored on other computers – banks, hospitals, online advertisers, data brokers, government agencies, and diverse other record holders possess exponentially more detailed data on individuals than in the past. Although a few people attempt to live "off the grid" (i.e., invisible to all recording systems), this is not a feasible option for the vast majority of citizens in developed countries. Once an individual is identified as a target, the government -- via lawful process -- can access detailed information specific to that individual.

We live in a "golden age for surveillance" because investigatory agencies have unprecedented access to information about a suspect. In addition, data mining provides unprecedented tools for identifying suspects. Law enforcement and national security agencies have built sophisticated data mining capabilities in-house, or can contract with the private sector for such capabilities.[129]

3. Choosing between "going dark" and "a golden age for surveillance." This paper argues that the big picture for agency access to data is mostly "golden" rather than "dark." The loss of agency access that encryption causes to some information is more than offset by surveillance gains from computing and communications technology. In addition, government encryption regulation harms cybersecurity and causes the least trusted country problem discussed above. These conclusions will not be easily accepted by investigatory agencies, however, so it is important to work through the analysis in more detail.

---

[128] See Peter P. Swire, "The Consumer as Producer: The Personal Mainframe and the Future of Computing," 42 Law/Technology, 1st Quarter 2009, at 8, note 3.

[129] [cite to DoD and other data mining studies; cite to private-sector offerings of data mining capabilities]

Law enforcement and national security officials face a very real problem today. Rapidly evolving communication technologies create difficult challenges for lawful interception. Communications that were previously subject to wiretap may now be shrouded in encryption. Agencies have to contend with new communications technologies, from social networks to video games.[130] In place of the old monopoly telephone network, agencies have to contend with a confusing variety of communications providers, some of whom have little experience in complying with legal process. It is no wonder that agency officials strenuously object the use of new technology that hinders their ability to employ traditional surveillance and investigative methods.

Implementing wiretaps and reading the plaintext of communications are not the only goal, however. The computing and communications infrastructure are vital to economic growth, individual creativity, government operations, and numerous other goals. If there is a modest harm to investigatory agencies and an enormous gain, then societies should choose the enormous gain. In 1999 the U.S. government concluded that strong encryption was precisely that sort of valuable technology – it was worth going at least slightly "dark" in order reap the many benefits of effective encryption. Not even the attacks of September 11, 2001 changed that judgment.

The evidence suggests, furthermore, that the degradation of wiretap capability has been modest at most, and at least statistically wiretaps have become more useful over time. The number of wiretap orders implemented in the United States has grown steadily in the last two decades. According to publically available statistics, court approved wiretaps are now at a record high.[131] 3,194 wiretap court orders were issued for the interception of electronic, wire, or oral communications in 2010, a 34% increase from the 2,376 issued in 2009.[132] In the six instances where encryption was encountered, the encryption did not prevent law enforcement from retrieving the plaintext forms of communication.[133]

These numbers actually understate the expansion of wiretapping in the U.S., in part due to the shift to "roving" wiretaps. In earlier years, separate court orders were required for each device used by the target of an investigation. Over time, however, Congress authorized roving wiretaps so that one wiretap order could apply to all the devices used by a suspect.[134] Instead of having multiple wiretap orders for a single suspect, roving wiretaps thus lessened the number of separate court orders reported in official statistics.[135] Additionally,

---

[130] Online video games, such as World of Warcraft, now incorporate chat and voice capabilities in the game. Although parents may complain about video games as a colossal waste of their kids' time, investigatory agencies see the video game in even more stark terms – a new international channel for terrorist and criminal communications. Yet the video games are not pre-cleared with government agencies before they hit the market. The sheer number and variety of communication technology thus continues to grow and at any given moment, some of those will not have an established method of access for law enforcement, even with a court order or other lawful process.

[131] The Omnibus Crime Control and Safe Streets Act of 1968 requires that the Administrative Office of the United States Courts annually report to Congress the total number of wiretap applications. 18 U.S.C. 2519(3).

[132] WT report p 7

[133] WT report p 9. Public law 106-197 amends 18 USC 2519 to require the inclusion of wiretaps for which encryption was encountered and whether those wiretaps prevented law enforcement form obtaining the plaintext of the intercepted communication.

[134] [cite statutes for ECPA and FISA]

[135] FN to year roving wiretaps laws established (look in Swire's FISA article for states) - The Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2518(11)) and the Intelligence Authorization Act of 1999

wiretaps over time were authorized by investigation, rather than for each individual target within an investigation. This similarly means that the statistics understate the growth in actual use of wiretaps.

What explains the agencies' sense of loss when the use of wiretaps has actually expanded, encryption has not been an important obstacle, and agencies have also gained all the new location, contact, and other information? One answer comes from behavioral economics and psychology, which has drawn academic attention to concepts such as "loss aversion" and the "endowment effect." "Loss aversion" refers to the tendency to prefer avoiding losses to acquiring gains of similar value.[136] This concept of loss aversion also helps to explain the "endowment effect" – the theory that people place higher value on goods they own versus comparable goods they do not own. Applied to surveillance, the idea is that agencies feel the loss of one technique more than they feel an equal-sized gain from other techniques. Whether based on the language of behavioral economics or simply on common sense, we are familiar with the human tendency to "pocket our gains" – assume we deserve the good things that come our way, but complain about the bad things, even if the good things are actually more important.

In addition to the behavioral economic perspective, there are institutional explanations for the focus on diminution in surveillance capabilities. Specific offices within government agencies are confronted with new obstacles to traditional wiretap techniques. These obstacles pose a threat to a specific office's influence or ability to do its assigned job. Offices that are affected in this manner have an incentive to object to changing capabilities, and do so by demanding new legal authorities or funding. Meanwhile, new surveillance capabilities may be developed within entirely different offices that take advantage of new technologies or do not face the same legal or technical challenges. Within an agency, therefore, the strongest institutional or political push quite possibly originates from the offices that face obstacles with the evolving surveillance landscape.

A related idea is that the agencies focus on one version of the status quo, where issuance of a court order led directly to access to the communications covered by the order. [137] That status quo is threatened if the communication is strongly encrypted or the communications are done within an online video game that lacks a way to comply with the court order. A different status quo, and the one emphasized here, is to look at the overall effects of computing and communications technologies on the agencies' ability to do their jobs. We have argued that these overall effects have assisted investigatory agencies greatly.

A simple test can help the reader decide between the "going dark" and "golden age of surveillance" hypotheses. Suppose the agencies had a choice of a 1990-era package or a 2011-era package. The first package would includes the wiretap authorities as they existed pre-encryption, but would lack the new techniques for location tracking, confederate identification, access to multiple databases, and data mining. The second package would match current capabilities: some encryption-related obstacles, but actual increased use of wiretaps, as well as the capabilities for location tracking, confederate tracking and data mining. The second

---

(18 U.S.C. § 2518(11)(b)) provide that prosecutors, upon showing probable cause, may use relaxed specification or "roving" wiretaps to target specific individuals by using electronic devices at multiple locations rather than a specific telephone or location.

[136] [cite on loss aversion] This theory was penned by Daniel Kahneman, who received the Nobel Prize for his work on loss aversion in collaboration with Amos Tversky.

[137] For an earlier version of this discussion of the status quo, see [Swire unpublished paper from 2000 Stanford Law Review symposium].

package is clearly superior - the new surveillance tools assist a vast range of investigations, whereas wiretaps apply only to a small subset of key investigations. The new tools are used far more frequently and provide granular data to assist investigators in both domestic and international investigations.

In conclusion, the 2011-era package is better than the 1990-era package. We are indeed in a golden age of surveillance, with investigatory agencies overall benefitting from computing and communications technology rather than going dark. Agencies' arguments about new deprivation are therefore unconvincing. In addition, the cost of implementing the agencies' proposals would be high. As discussed already, strong encryption is vital to overall cybersecurity and limits on encryption create the least trusted country problem. The partial degradation of one law enforcement tool should not become the basis for undermining those other vital interests.

C. Domestic Industry, Trade Policy, and Encryption

Every nation's trade policy affects its position on encryption. At a basic level, U.S. industry in the 1990s supported strong encryption, whereas at least some portions of Chinese and Indian industry may benefit from limits on strong encryption. This section will briefly discuss trade policy considerations for these three countries. We conclude that the global importance and inherent value of strong encryption should take precedence over local trade concerns.

1. U.S. Encryption and Trade Policy in the 1990's. During the 1990s, U.S. software and computing companies were the leaders in the spread of the Internet. Microsoft, Oracle and Sun Microsystems were pioneers in the global software market, Intel and Cisco led the way on microprocessors and routers, and IBM and others were prominent in online services. For these companies, export controls on encryption were a competitive threat. Foreign competitors were able to sell strong encryption without being subject to U.S. export controls, and success of these competitors in encryption might be an entering wedge for broader success for the non-U.S. companies. U.S.-based companies increasingly considered locating production abroad, also to avoid the export controls. This harm to U.S. industry, together with the futility of restricting access to strong encryption, contributed to Congressional and other political support for strong encryption.

Over time, a more subtle policy issue garnered attention. The U.S. military and other government entities wanted to have access to the best encryption in the world for use in their own systems. Having the cutting-edge encryption go abroad would threaten those systems' security. The NSA's preference for effective wiretaps thus conflicted with the U.S. military's desire to maintain a strong U.S. encryption infrastructure. Early in the 1990's, the political lineup featured an alliance between the Department of Justice, the FBI (which reports to Justice) and NSA, opposed primarily by the Department of Commerce.[138] Over time, the Pentagon, which is the parent agency to the NSA, shifted towards a view that limits on strong encryption would harm the military. This analysis is consistent with the statement of Deputy Secretary of Defense Hamre when he said: "We are just as vulnerable in cyberspace as is anybody, and we strongly need the sorts of protections that come with strong encryption."[139]

[138] This discussion draws on Swire's experience in government during this period.
[139] *Supra* note __.

By 1999, the explosive growth of the Internet and E-commerce made the commercial importance of encryption evident to a wide range of policymakers. Trade policy thus supported the shift in policy toward strong encryption.

2. China trade policy today. In contrast with the detailed known history of the U.S., there is less documentation about China's encryption policy. At least two commercial objectives appear to motivate China's insistence on domestically produced cryptosystems. First, China hopes to foster the transfer of encryption technology to its country. China's Policy on Indigenous Innovation is intended to reduce Chinese dependence on foreign technology and requires technology transfer as a condition to participating in the government procurement process.[140] Foreign companies wishing to conduct business in China, therefore, must consider the risks that their cutting-edge technologies will be accessible to the government and will potentially be made available to future Chinese competitors.

Second, China's push for homegrown encryption algorithms underscores their desire to lead the global encryption export market. By mandating the use of Chinese produced encryption algorithms within the country, China hopes to establish a substantial market for homegrown encryption. If Chinese encryption products and services do reach industrial scale within China, they have a greater chance of obtaining a large share of the global encryption market. The current Chinese strategy thus may launch a new export market, based both on the transfer of encryption technology into China and achieving industrial scale to support low cost exports to the rest of the world.

As a matter of international trade policy, this approach has encountered severe criticism. First, the policy is inconsistent with the sprit of free trade under the World Trade Organization, which China joined in 2001. The Policy acts as a major barrier to international trade and has no counterpart in any of China's trade partners.[141] The U.S. Chamber of Commerce and others have decried China's Policy on Indigenous Innovation over concerns that Chinese companies are favored over foreign operators. Second, the mandate for foreign companies to transfer technology is particularly vexing given the ongoing concern of piracy - China does not adequately enforce intellectual property rights, including in patents. Third, the mandate to use only Chinese produced encryption violates the norms and possibly the international trade rules ensuring fair competition in government contracts.[142] Fourth, these concerns are exacerbated by the risk that subsidies will be provided to Chinese manufacturers over foreign operators. These subsidies themselves contradict international trade obligations. In the United States, for example, such subsidies can be the basis for countervailing duties and other trade sanctions.[143] The U.S. and other countries continue to object to China's Policy, though minor changes have resulted from negotiations thus far.

---

[140] U.S. Chamber of Commerce, China's Drive for "Indigenous Innovation"-A Web of Industrial Policies (2010).
Available at http://www.uschamber.com/reports/chinas-drive-indigenous-innovation-web-industrial-policies.
[141] SuYuan An and Brian Peck, China's Indigenous Innovation Policy in the Context of its WTO Obligations and Commitment, Georgetown Journal of Int'l Law Volume 42, 375 (2011), available at http://gjil.org/wpcontent/
uploads/archives/42.2/ChinasIndigenousInnovation.pdf
[142] [Cite to Steve Schooner on international procurement]
[143] [cite to countervailing duty law]

Even more compelling than international trade issues are the cyber security and encryption policy implications of China's approach. The most troubling aspect of their encryption policy is that Chinese developed cryptosystems have not undergone a fraction of the testing major global encryption standards are subject to. As discussed above, "[c]ryptography is fiendishly difficult. Even seasoned experts design systems that are broken a few years later."[144] In the absence of any theoretical proof of cryptosystem strength, resistance to repeated empirical testing is the most important indicator of trustworthiness. A legal mandate to use a lightly tested cryptosystem, therefore, creates a substantial risk that the cryptosystem will be broken upon deployment. Without such testing, reputable cryptanalysts are likely to dismiss the encryption standard as unreliable, thereby undermining the goal of establishing a legitimate and widely used encryption standard.

It is also unwise to build potentially weak components into hardware and software used within China and exported abroad. If such software or hardware relies on a cryptosystem that can easily be broken, the data and communications protected by those systems will be compromised. It is true that software can be patched once vulnerabilities are discovered;users, however, users are notoriously slow in installing patches. Additionally, systems relying on earlier versions of the software may have already surrendered the security of their data. This problem is even more acute if the weak cryptosystem is implemented in hardware, such as computer chips. Hardware has the potential to be incorporated into an enormous array of devices, including sensitive communication devices or critical infrastructure. Hardware, however, is typically much more difficult to patch than software. Though software patches involved cumbersome downloads, actual physical replacement may be required for the compromised hardware. Special care must be taken to mitigate the risks associated with hardware vulnerabilities that may persist throughout the life of the flawed device.

Use of lightly tested cryptosystems also makes it virtually impossible for observers outside of China to assess the risk of backdoors. Global cryptosystems such as AES and open implementation libraries such as SSL and CryptoAPI have been subjected to a wide variety of attacks. Experts from numerous nations have thoroughly tested standards such as AES; indeed, two Belgian cryptographers, Joan Damien and Vincent Rijmen, developed the AES cipher that later won a security competition at the NSA.[145] Early weaknesses have been now been fixed and today the system is stable. Thus, as discussed above, it seems highly unlikely that there is a backdoor to AES. By contrast, however, the Chinese cryptosystems have not been subjected to the level of scrutiny that would lead a fair-minded observer to conclude backdoors do not exist. Without wishing any disrespect for the computer scientists who develop these new cryptosystems, it is disconcerting that so many high profile computer attacks appear to originate in China. When persistent and sophisticated attacks originate from a particular source, concern that attackers are using the new cryptosystems as a Trojan horse into global computer systems is understandable.

Even if no backdoors exist, there is also the possibility that cyber attackers in China will develop a tradecraft in breaking cryptosystems. This tradecraft may result from recurring opportunities to both install and attack cryptosystems as they are used in China. Tradecraft may also emerge from collaboration or a shared computing culture between the designers of cryptosystems and those who attack the systems outside of China.

Chinese insistence on employing lightly tested cryptosystems thus faces strong objections on both trade and cyber security grounds. This paper emphasizes the latter. International standards for encryption are based on the principle of open and widespread testing as the empirical foundation for trustworthiness. Even if the most

[144] Schneier, Ferguson, Kohno, Cryptology Engineering, at 13.
[145] AES creators

skilled programmer in the field creates a cryptosystem, the collective public is the best tool for evaluation. Encryption developed in a closed environment may also foster distrust and fear that system vulnerabilities are being hidden, or that user privacy will be compromised by way of secret backdoors. At a time when encryption is an integral component of global communications, one country should not insist on inserting weak encryption into computing systems. A country-specific approach to encryption not only raises costs for consumers and companies who must integrate their operations with standards that are not globally accepted, but also systematically reduces the overall security of the Internet, hardware, and other important aspects of computing.

3. India trade policy today. The international trade situation in India today is broadly similar to that in the U.S. during the 1990s. India's business process outsourcing (BPO) sector now accounts of over X billion dollars in revenue annually and is over Y% of India's GDP.[146] Back office operations are extensively used by many industries including insurance, health, telecommunications, banking, and others that regularly handle sensitive personal information.

Weak encryption, however, threatens future growth of India's BPO sector. Suppose, for example, that health insurance companies or hospitals in the U.S. or Europe were considering sending medical records to India for customer service and other back office operations. If Indian law mandates the use of weak encryption, those medical records cannot lawfully enter India in a secure manner. The exporting companies may then face domestic sanctions and penalties for weak security and privacy practices. In addition, India's foreign competitors can use Indian encryption laws as a persuasive reason for attracting business to their countries. This is not hypothetical - the American Recovery and Reinvestment Act of 2009 sets aside $19 billion in financial incentives for U.S. companies to adopt certified electronic health record (EHR) technology. Current standards require the EHR technology to employ strong encryption.[147]

More generally, the Indian BPO sector must abide by the laws of various countries requiring cost effective security measures. The European Union Directive on Data Protection requires "adequate" protection of personally identifiable information that is transferred outside of the E.U. The Directive includes an expectation of computer security.[148] In the U.S., the Gramm-Leach-Bliley safeguards rule similarly requires the implementation of risk-based security measures. Given the relatively low cost and high strength of commercial encryption today, regulators and BPO competitors outside of India have a strong argument that weak encryption in India violates such security laws.

Other India trade policy concerns surround the issue of technology transfer. Similar to China and other developing nations, India would like to foster technology transfer and training of its domestic workforce to global standards of competitiveness. India thus has an incentive to negotiate and encourage global companies to build facilities within India and to train Indian workers. This push for technology transfer is significant with

[146] BPO statistics

[147] 45 CFR §170.302. General certification criteria for EHRs requires that electronic health information be encrypted and decrypted in accordance with §170.210(a)(1) and (a)(2) unless the use of such encryption would pose a significant security risk for Certified EHR Technology.

[148] (FN – cite to the directive India is in the midst of implementing a new data protection law. One of its major goals is meeting the adequacy requirement of the E.U. directive. The point made here is that no set of privacy policies can be considered adequate if they are implemented in a known and thoroughly insecure manner, such as lacking encryption for international transfers of personal data. Here also have some recent law stories about the Indian data protection law, what the law requires, etc.)

regards to the telecommunications and computing sector. Unlike China, India thus far has not pushed for the production and export of domestic encryption. India, instead, may be leaning towards installing import controls on encryption. The impetus for such controls would stem from Indian law enforcement and national security agencies concerns. These agencies, in hopes of retaining wiretapping capabilities, have an interest in enforcing a ban on the import of strong encryption. Such controls could require an import license that certifies compliance with India's encryption laws.

There are numerous and compelling arguments against the use of such import controls. Such controls are questionable as a matter of trade policy and would need to pass muster under World Trade Organization and other applicable trade laws. Moreover, imposition of a potentially burdensome licensing regime underscores the untenable nature of bans on effective encryption. India would be mandating weaker security for its computing and telecommunications sectors, thus holding those sectors behind in the race for global competitiveness. These import controls are not only ineffective trade policy but would likely face the same futility arguments that were important during the U.S. crypto debates in the 1990s. As was true in the 1990s, today strong encryption is easily downloadable from points outside the country. Once again, malicious actors would have access to effective encryption while legitimate actors would be trapped with poor cybersecurity.

4. Summary on Trade Policy Considerations. The strongest cryptosystems today are the subject of constant and sophisticated testing by an international community of experts. National laws that depart from international standards lead to weaker cybersecurity, not only for the nation promulgating the laws, but also for the rest of the world. In the name of assisting domestic industry, countries may be tempted to rely on homegrown encryption; however the discussion above illustrates that this approach violates both international trade norms and the goals of cybersecurity. Efforts by law enforcement and national security agencies to limit effective encryption are also subject to grave doubt. Other countries may be tempted follow one of these paths. Such efforts are harmful as a matter of trade policy and may cause irreparable damage to the security of global computing and communications.

V. Theoretical Model and Policy Prescriptions for when Strong Encryption should apply

[This policy discussion is in preliminary form – perhaps too preliminary to be worth sharing at this point. The key question for readers is the usefulness of the proposed 2x2 matrix, which shows reasons why strong encryption should be encouraged for Cell 4 of the matrix, where the channel of communication is insecure and agencies can seek access to stored records after the fact. By contrast, Cell 1 is for the classic phone wiretap situation, where the channel is secure (a well-run telephone network) and the information is transitory and thus not available after the fact.

In the next edit of the paper, more attention will be given to Susan Landau's recent book. She argues that CALEA-style regulation creates systematic vulnerabilities in the communications network, and that surveillance thus causes large security risks. If Landau is assumed to be correct, then even Cell 1 regulation may well be undesirable. Even on that assumption, the argument for strong encryption in Cell 4 situations is even more compelling.]

To date, incongruous policy decisions have been made regarding law enforcement and national security access to communications. The 1994 passage of CALEA preserved the ease of lawful access to communications transmitted over the traditional telephone network. However, the 1999 shift in U.S. policy favored widespread adoption of strong encryption for Internet communications. It is possible that these policy shifts were the result

of power politics, in which government agencies prevailed in 1994 but lost in 1999. This paper, however, asserts that an intellectual coherence exists between these seemingly disparate shifts in policy.

There are two dimensions that illustrate the distinction between the CALEA outcome, for the phone network, and strong encryption for the Internet. The first dimension concerns the security level of the channel of communication. As discussed above and as illustrated in Figure 3, the Internet operates on a fundamentally unsecure architecture, in which unknown and malicious nodes can potentially intercept communications traveling through the network. By contrast, the telephone network is a unified transmission system under the control of one (or a few) large telephone providers. In the telephone network, untrusted parties generally do not have access to traveling communications. Although various forms of penetration may be possible, the working assumption is that the telephone company itself controls the network. Thus, a traditional telephone network is "trusted" and "secure" while the Internet structure is "untrusted" and "unsecure."

The distinction between a secure and unsecure network has direct implications for encryption policy. Effective encryption is essential for protecting communications sent over an unsecure network. Otherwise, malicious attackers must be presumed to have access to all communications. By contrast, encryption is not necessarily required when the network itself is considered secure. Assurances of security, in that instance, depend on the actions of the telephone company that controls the network. Legal, technical and administrative safeguards may be used to avoid the complexity associated with implementing strong encryption.

The second dimension concerns the relative amount of time needed to access transitory data versus stored records. As its name suggests, transitory data leaves a fleeting digital footprint; once the call has ended, there is no further possibility for law enforcement to gain access to the communication. Therefore, law enforcement and national security agencies need the ability to implement a wiretap immediately in order to capture the information. By contrast, records sent through the Internet are often stored by communicating parties as well as Internet service providers. To access emails and other stored records, law enforcement can obtain a court order after the communication has been sent and use it to retrieve the record.

Using these two dimensions, Figure 6 illustrates when law enforcement and national security agencies have a stronger or weaker case for restricting encryption. In this 2x2 matrix, the vertical axis represents the relative level of network security, ranging from "secure" at the top of the axis, to "unsecure" at the bottom. The horizontal axis represents the type of communication, ranging from entirely "transitory" communication on the left to "stored" communication on the right. The CALEA framework applies in the Cell 1 scenario wherein transitory communications are sent through a secure network.

At the other end, the Cell 4 scenario corresponds with the encryption debates resolved in 1999. In this scenario, stored records, such as emails, are being sent over an "unsecure" network (the Internet). The risks of sending unencrypted communications in the cell 4 environment are great. Meanwhile, the potential loss of access for law enforcement purposes is distinctly lower. If the agencies do not access the communications during transit, they can use lawful process to retrieve the records from storage.

The scenarios represented in the 2x2 matrix mirror the outcomes of the debates on encryption in 1999 and lawful access in the 1990s. The matrix scenarios are also normatively attractive. Law enforcement and national security interests are most urgent when the communication is transitory, and where the network itself poses low risk of attacks, thereby lessening the need for strong encryption. Law enforcement concerns are less urgent

when the communications are stored and sent over an unsecure channel. In this scenario, encryption is necessary to protect communications over the unsecure network, but will not hinder law enforcement access.

A. Applying the 2x2 Matrix

The real world, of course, does not fit perfectly within a 2x2 matrix. Ideally, communications covered by cell 1 would travel through an entirely secure telephone network. Legal, technical and administrative controls would prevent any unauthorized access to those communications. In practice, however, these controls may not provide effective deterrence against efforts to penetrate and access communications. Wire tappers and other telephone hackers may succeed in some instances and the administrative safeguards may not prevent unauthorized access by telephone employees, law enforcement agents, or others malicious actors.

Similarly, a continuum exists between entirely transitory and entirely stored records. Even voice communications, depending on network configuration, may be cached or otherwise stored at intermediate locations, if only for a short time.[149] In addition, certain records that are typically stored might be deleted or physically destroyed. Although emails and other stored communications are often difficult to delete completely, determined efforts could result in completely erased communications. Even where storage exists, legal, technical, or other barriers may prevent an agency form determining who holds the records, or enforcing a court order to obtain those records.

Although communications may not be transmitted through entirely secure or insecure networks, or remain in entirely transitory or stored stages, the matrix nonetheless provides a parsimonious means of understanding where law enforcement limits on encryption are most justified.

Intermediate cases exist when one of the two criteria points in each direction – i.e. the network is untrusted and the communication is transitory or stored, or the network is secure and the communication is transitory or stored.

VOIP is a prominent example of an intermediate case in which the communication is traveling through an untrusted channel (the Internet) and is generally transitory in nature, but in some instances may be stored. Depending on the network architecture, the bits that use IP for VOIP may be cached between Alice and Bob. To the extent those bits are stored over time, the voice communication is not entirely transitory. For most VOIP communications, however there is no long-term storage of these bits. That lack of storage militates in favor of the preserving real time access for the agencies. The problem with this approach, however, is the thoroughly insecure nature of the Internet. Prohibiting or even limiting the use of encryption would make wiretapping trivially easy for third parties. The insecure nature of the Internet distinguishes VOIP communications from typical voice communications sent over the traditional telephone network. For this reason, CALEA should not be applied universally to VOIP communications.

Some situations may exist where the network is relatively secure but the records are stored, in which case the justification for real time lawful access is weak. For example, faxes were traditionally transmitted through the phone network. The fax print out is a stored record that is subject to lawful process after it has been received. Another example is a physical record that is stored and secured by physical measures instead of encryption. In these cases, use of encryption is not as critical as it is for data sent over insecure networks.

[149] For discussion about such caching for VOIP communications see [cite Swire testimony]

B. Policy Implications of the Matrix

Justification for limits on encryption appears stronger for the cell 1 than for cell 4. In cell 1, the network is secure and hackers do not pose a significant threat. The communication is transitory, however, which increases the urgency for providing real time lawful access. In this case, limitations on encryption are understandable. In cell 4, the insecure nature of the network increases the need for encryption. Law enforcement can access the stored communication after transmittance, making justifications for encryption limitations weak.

With that said, however, situations may exist where encryption is always necessary, or when limits on the use of encryption are always necessary. Defenders of strong encryption might find CALEA-like restrictions for the Internet highly objectionable. Similarly, proponents of CALEA may believe that wiretap readiness mechanisms should apply to all Internet communications. Despite these potential scenarios, this matrix provides useful framework for determining which issues are at stake in different settings.

This paper has analyzed many of the arguments in favor of using strong encryption for all communications sent over the Internet, the most prominent being the effectiveness of encryption as a cyber security tool, and the grave risks associated with the "least trusted country" problem. In terms of the provided matrix, the cell 1 justification for encryption limits may actually be weaker than it appears. The ideal cell 1 scenario assumes that the telephone network is secure. Today, however, modern international telephone communications resemble the multi-node Internet network. If Alice makes an international call to Bob, her communication is exposed to more points of potential compromise than ever before.

As international communications proliferate, the "least trusted country" problem becomes increasingly applicable to telephone communications. The "going dark v. golden age of surveillance" discussion highlights the point that public policy should avoid mandating wiretap readiness when possible. The many tools now available to agencies make traditional wiretaps a far less significant fraction of surveillance capabilities than before, and the quantity of stored records makes the need for real time lawful intercept much less urgent.

The matrix also helps call attention to macro trends in global communications. Generally, communications are shifting from scenarios in Cell 1 to those in Cell 4. This shift reflects the evolving capabilities of the digital space - from sharing emails and texts, to videos, and photographs - which have made the Internet our preferred medium of communication. Traditional telephone carriers are responding by making greater use of Internet protocol networks.[150] As more of our interactions take place over unsecure channels, total stored communications increase at a staggering rate. This inexorable trend towards Cell 4 communications bolsters the case for strong encryption.

C. The Importance of Lawful Access Rules

Whether a communication is treated as "transitory" versus "stored" depends on the effectiveness of lawful process. Imagine that law enforcement and national security agencies have well established and effective mechanisms for obtaining stored records upon legitimate legal process. Today, communications are often stored, lessening the need for real time wiretap capability. Now imagine there are no effective or practical means of obtaining those stored records after transmittance. In this case, there is no real distinction between

150

stored and transitory records – i.e. the existence of stored records does not translate into automatic access for law enforcement upon legal process.

In the U.S. and other countries, government agencies do have effective legal means of accessing stored records. In the U.S., the Electronic Communications Privacy Act (ECPA) provides access to emails and other electronically stored records, while the Foreign Intelligence Surveillance Act (FISA) provides access to records for national security purposes.[151] Roughly analogous rules exist under the Counsel of Europe's Convention on Cybercrime. This paper does not challenge nations' rights to access stored records through a well-established legal or judicial system. [152]

Cross border access to records, however, is more challenging. Indian officials, for instance, have expressed concern about their inability to obtain records stored in the U.S. One mechanism for facilitating transborder requests is through a mutual legal assistance treaty (MLAT). India and the U.S. signed an MLAT agreement in 2005 providing a transparent legal basis for the transfer of stored records between the countries.[153] More generally, the European Convention on Cybercrime also regulates these types of transborder data requests. The effectiveness of MLATs in facilitating these requests deserves further study and may be a promising avenue for future agreements between nations.

Ideally, the MLAT process would enable lawful access upon a proper evidentiary showing, while blocking phishing expeditions and preventing intrusions. The establishment of an effective legal process is far preferable to other alternatives. As discussed above, key escrow and other limits of effective encryption result in extensive network vulnerability.

Conclusion

[Add conclusion]

[151] PS article FISA, Orin Kerr on ECPA

[152] This paper does not take a position on the precise standards that should apply for ECPA and FISA. In the past, Peter Swire has written extensively about the need for ECPA and FISA to be tailored in order to protect against excessive surveillance. The purpose of this paper is to instead describe how some lawful process systems are the corollary for treating stored records differently than transitory communications under wiretap laws.

[153] FN describing procedures from MLAT India/U.S.

Appendix

FIGURE 1

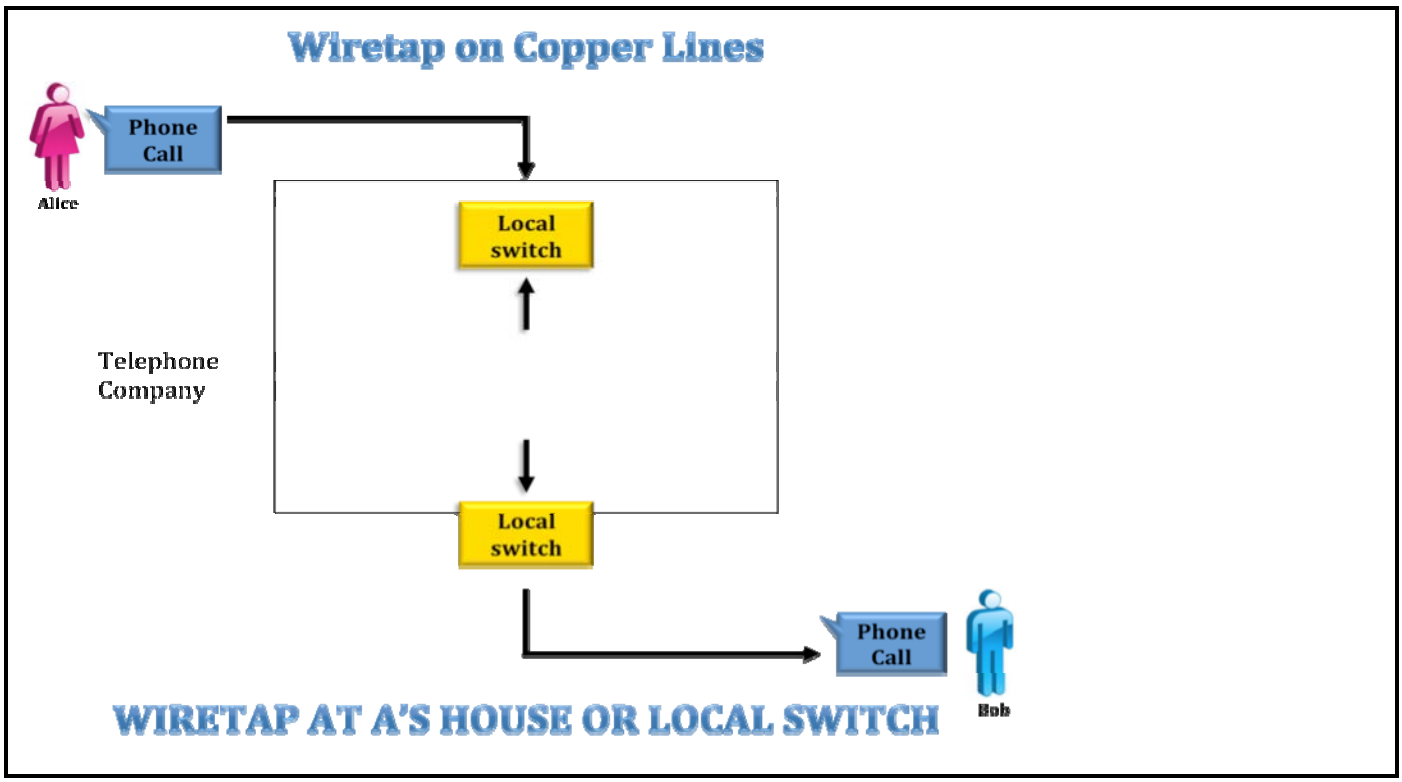


FIGURE 2

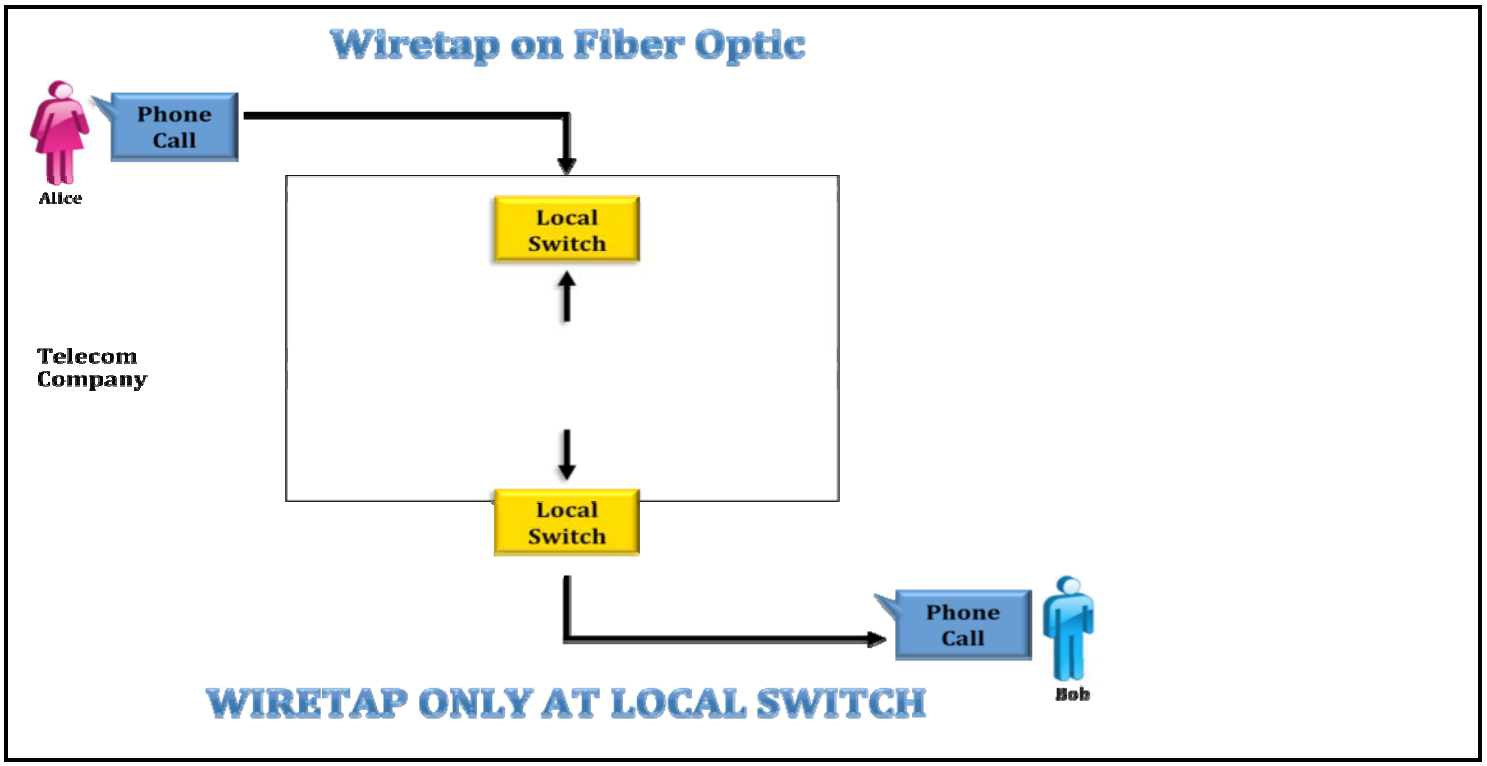

Wiretap on Fiber Optic
Phone Call
Alice
Local Switch
Telecom Company
Local Switch
Phone Call
Bob
WIRETAP ONLY AT LOCAL SWITCH

FIGURE 3

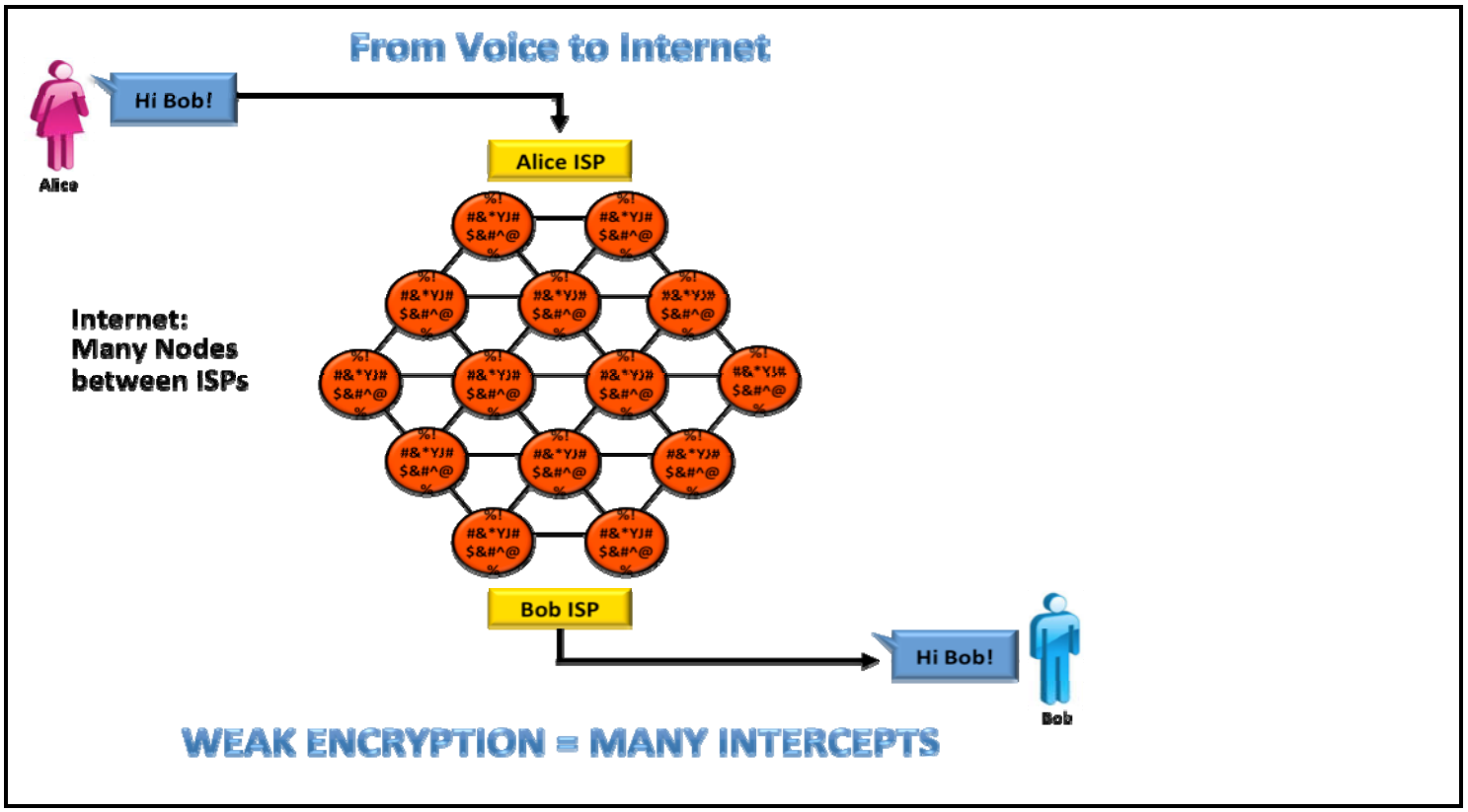

From Voice to Internet
Hi Bob!
Alice
Alice ISP
Internet:
Many Nodes
between ISPs
Bob ISP
Hi Bob!
Bob
WEAK ENCRYPTION = MANY INTERCEPTS

FIGURE 4 - GEODESIC DOME

FIGURE 5

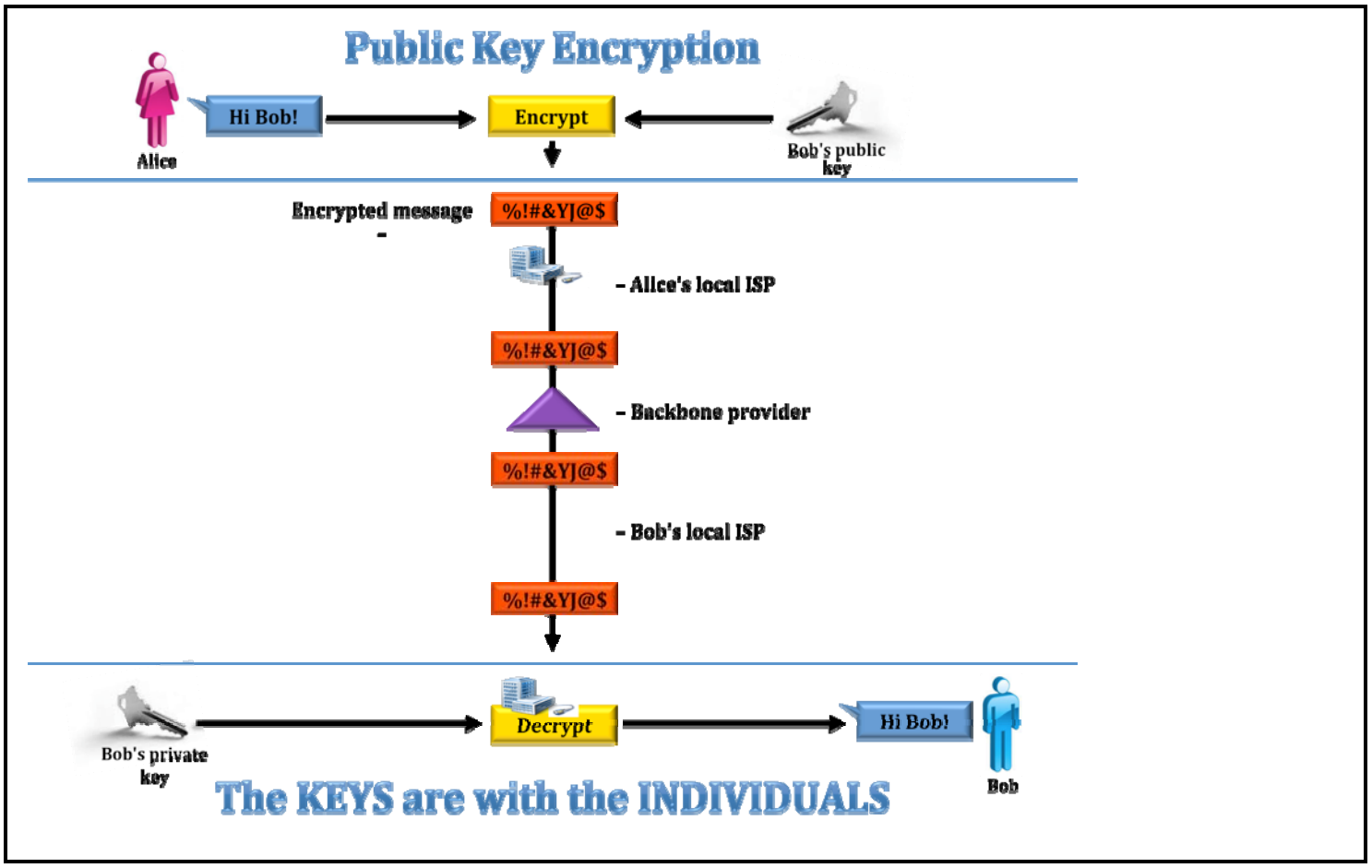
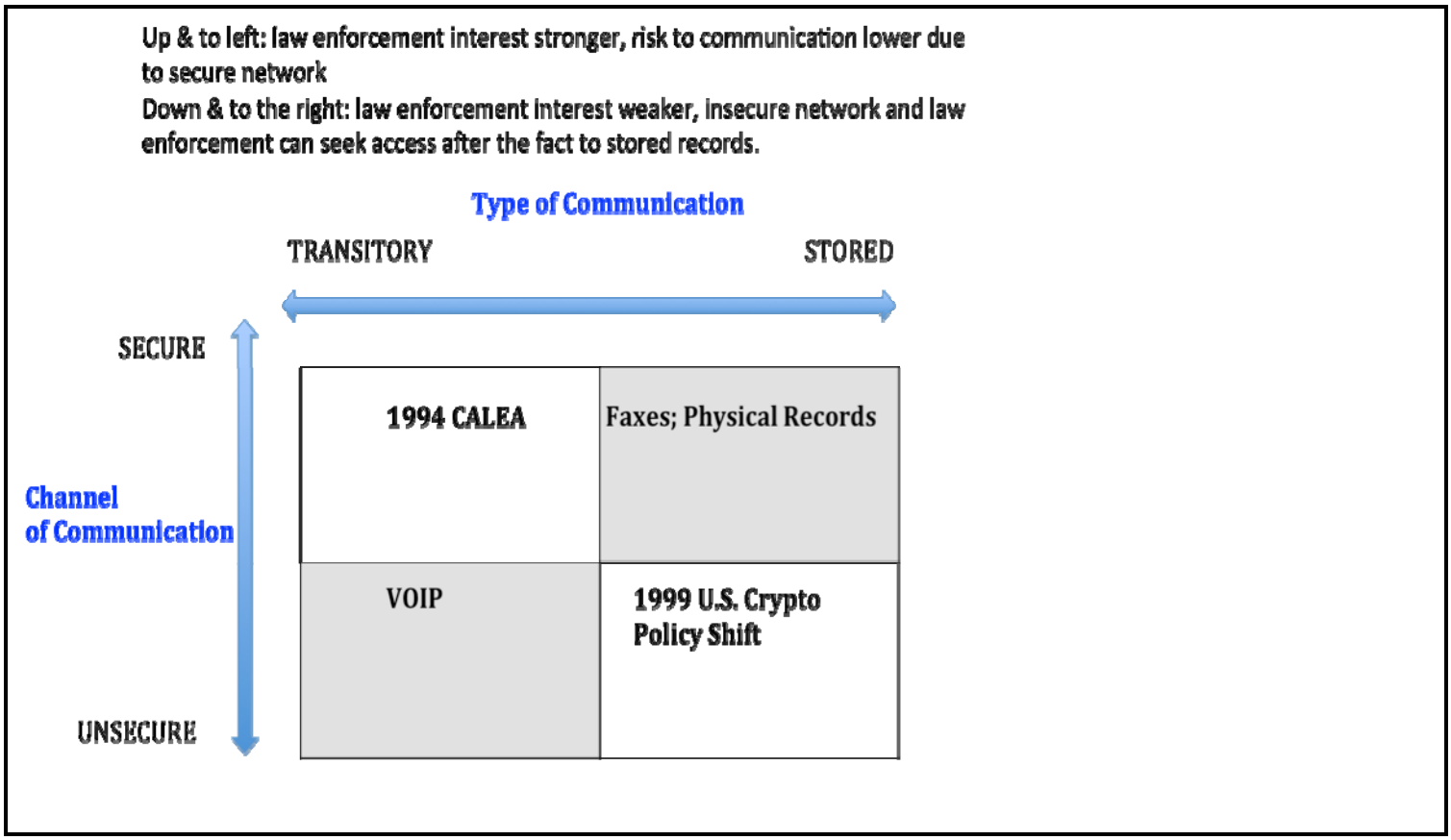

Public Key Encryption
Alice
Hi Bob!
Encrypt
Bob's public key
Encrypted message
%!#&YJ@$
- Alice's local ISP
%!#&YJ@$
- Backbone provider
%!#&YJ@$
- Bob's local ISP
%!#&YJ@$
Bob's private key
Decrypt
Hi Bob!
Bob
The KEYS are with the INDIVIDUALS

FIGURE 6


Up & to left: law enforcement interest stronger, risk to communication lower due to secure network
Down & to the right: law enforcement interest weaker, insecure network and law enforcement can seek access after the fact to stored records.
Type of Communication
TRANSITORY
STORED
SECURE
Channel of Communication
UNSECURE
1994 CALEA
Faxes; Physical Records
VOIP
1999 U.S. Crypto Policy Shift