THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XIII STLR.ORG SPRING 2012

ARTICLE

ENCRYPTION AND GLOBALIZATION[†]

Peter Swire[*] and Kenesa Ahmad[**]

During the 1990s, encryption was one of the most hotly debated areas of technology law and policy. Law enforcement and security agencies initially supported limits on the export of strong encryption for national security reasons. In 1999, however, the administration shifted position to allow largely unrestricted export of encryption technologies. Encryption law and policy discussions largely faded from view.

Recently, encryption is again resurfacing as a major point of policy discussion. Changes to Indian and Chinese laws regarding encryption technologies have raised questions of international trade, national security, and communications security.

There are key lessons learned from the U.S. experience that are highly relevant when the debate shifts from one country to a globalized setting. However, since the U.S. encryption question was settled in 1999, a new generation of policy makers, lawyers, and technologists

[†] This Article may be cited as http://www.stlr.org/cite.cgi?volume=13&article=9. This work is made available under the Creative Commons Attribution–Non-Commercial–No Derivative Works 3.0 License.

[*] 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 chair of the White House Working Group on Encryption in preparation for the Clinton Administration's 1999 announcement that it would support strong encryption. For financial support, the authors thank the Future of Privacy Forum, Google, Intel, Microsoft, and the Moritz College of Law. The authors express thanks for comments on versions of this Article at Financial Cryptography '12, the Intellectual Property Scholars Association 2011 conference, and a Moritz College of Law Workshop, as well as at presentations to government and industry experts in the United States and India. Thanks in addition to Stewart Baker, Audrey Plonk, Bruce Schneier, Chris Soghoian, Claire Vishik, and others.

[**] Kenesa Ahmad received her J.D. 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 LL.M. from Northwestern University Law School. She is currently a Legal and Policy Fellow with the Future of Privacy Forum.

has emerged with little or no experience in the area of encryption policy.

This Article seeks to fill an important gap in the literature, and to inform the debate on encryption policies in the face of increasing globalization. By examining the relevant history, technology, law, and policy, this Article explains why it is vital to assure the widespread and global availability of strong encryption for our data and communications.

INTRODUCTION

During the explosive growth of the Internet in the 1990s, encryption was quite likely the single most passionate area of legal and policy debate. Broadly speaking, law enforcement and national security agencies supported limits on the export of strong encryption, fearing that encryption would block their vital ability to protect public safety and national security. On the other side, supporters of strong encryption included most information technologists, high-tech companies, and civil liberty and privacy groups. These supporters wanted encryption for many reasons, but most basically because they believed that encryption was essential to securing communication over the Internet, where numerous operators of the network could otherwise read unprotected communications.

The United States "crypto wars" of the 1990s proceeded in three main stages. First, law enforcement and national security agencies prevailed in imposing strict limits on effective encryption. Second, the Clinton administration proposed the controversial "Clipper Chip," in hopes of enabling both strong encryption and access by law enforcement pursuant to court order, using a "key escrow" system. Third, the administration shifted position in 1999, accepting the essential role of encryption for the Internet, and allowing its export without restrictions. After this shift in policy, encryption law and policy largely faded from view, and there has been very little legal or policy discussion of these issues in the past decade.

Encryption is now resurfacing as a major issue, most visibly in India and China, but also in Russia and a wide range of other countries outside of Europe and North America. Indian law currently forbids the use of encryption keys longer than 40 bits, which is far below international standards. Front pages around the world have reported on efforts by the Indian government to require Research in Motion (RIM) to change its architecture to enable wiretaps of encrypted Blackberry messages. China has also departed from global encryption standards. To support local industry and promote eventual exports, China now insists that hardware and software made or used in China only employ cryptosystems developed in China. These systems have not been subject to the rigorous peer review process required for international standards. In addition to significant international trade objections to this approach, there are serious security concerns about implementing these homegrown encryption products into in the global supply chain.

This Article seeks to fill an important gap in the literature. Because the U.S. encryption problem was "solved" in 1999, a new generation of policy makers, lawyers, and technologists has emerged with little or no experience in the area of encryption policy. As debates about encryption spring up in India, China, and elsewhere, there is no source that pulls together the relevant history and background, and explains the implications for today's encryption debates.

Good encryption policy results from a mix of history, technology, policy, and law. Part I of this Article offers a short history of wiretaps for phone and Internet data, illustrating why communications across the Internet are far more vulnerable than traditional phone calls, unless encryption is used. Part II provides a primer on basic encryption concepts that are relevant to the subsequent legal and policy analysis. The discussion assumes no prior knowledge of the topic.

Part III highlights key lessons learned from the U.S. crypto wars of the 1990s, informed by the perspective of one of the authors, who chaired the White House Working Group on Encryption in the lead-up to the 1999 change in U.S. encryption policy. This history includes an explanation of the major technical and other flaws in the key escrow approach, such as that attempted with the Clipper Chip proposal.

The U.S. encryption debates provide highly useful background for the current global encryption debates. In addition to highlighting the most compelling arguments from the U.S. experience in the 1990s, the Article proposes two additional reasons why effective encryption becomes even more important when the debate shifts from one country to a globalized setting. The first is the large and growing importance of cybersecurity for nations around the world. In cybersecurity today, the "offense" (in the form of thousands of attacks per day) is significantly ahead of the "defense" (in the form of tools and systems deployed by individuals and organizations to protect their data). Cryptography has become deeply integrated into all aspects of computing since the 1990s, and is today the single most important category of cybersecurity tools. In an increasingly interconnected and globalized world, security holes in one country (such as India or China) directly lead to security holes elsewhere.

The second reason why encryption is especially important for globalization is what we call the "least trusted country problem." The U.S. encryption debates during the 1990s focused primarily on the best policy for one nation, the United States. A repeated criticism of the Clipper Chip was the lack of trust that the United States would escrow the encryption keys securely, or use its decryption powers wisely. In a globalized setting, the consequences of limiting encryption are much more dire if key escrow or other limits are imposed in a dozen, 50, or 200 countries. How much trust would India place in its communications in the hands of Pakistan, China in the hands of Taiwan, and so forth? As the debate shifts from a setting of one to many nations, the level of trust placed in data traveling through the Internet becomes that of the country that we trust least.

Part V addresses major criticisms voiced by those who wish to limit use of effective encryption. Notably, law enforcement and national security agencies fear they are "going dark" as criminals and terrorists increasingly use a bewildering variety of new communications tools. On more careful examination, however, this Article contends that this mix of new technology is actually enabling a "golden age of surveillance." Understanding the enormous surveillance capabilities coming into the hands of agencies, rather than focusing on the manageable obstacles created by encryption, is important to reaching an accurate conclusion about the overall need for strong encryption.

This Article concludes by synthesizing the key reasons supporting effective encryption in today's globalized world, despite the security objections of law enforcement and national security agencies, and the trade interests of some countries. By examining the relevant history, technology, law, and policy, this Article explains why it is vital to assure the widespread and global availability of strong encryption for our data and communications.

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.[1] Originally, wiretaps were conducted through copper telephone wires. In this scenario, Alice would make a phone call to Bob, as illustrated in Figure 1.[2] 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.

[1] *See generally* Paul Rosenzweig, *Cyberwarfare: How Conflicts In Cyberspace Are Challenging America and Changing The World,* 12 J. Federalist Soc'y, (forthcoming 2012) (providing a basic history and policy discussion of wiretapping and encryption in the United States).

[2] The names Alice and Bob were first used in the seminal paper on public-key encryption. Ron Rivest, Adi Shamir and Leonard Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 21 Comm. of the ACM 120 (1978).

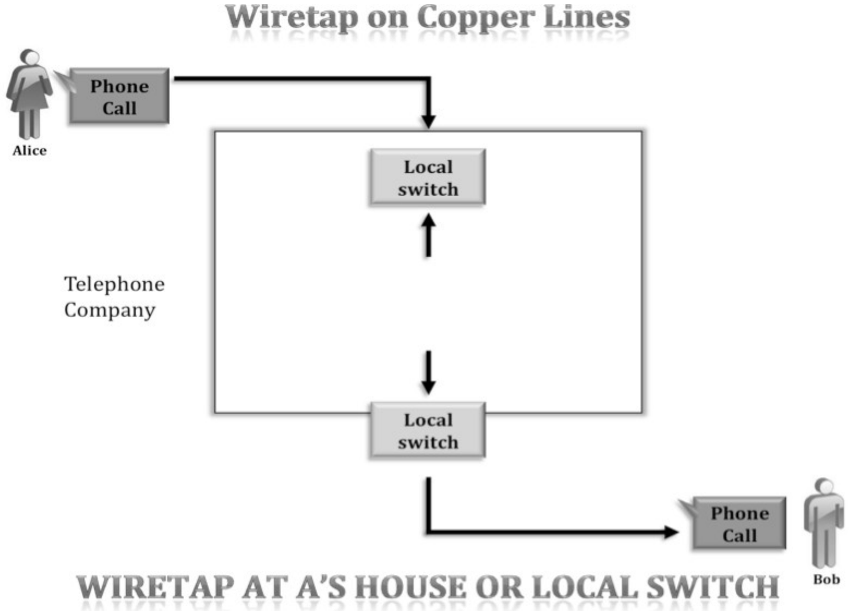

Figure 1. Copper Line Wiretapping

The approach to wiretapping shifted dramatically with the widespread adoption of fiber optic lines in the early 1990s. Figure 2 illustrates this change 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 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. The change from copper wires to fiber optics in telephony thus created a difficult challenge for law enforcement agencies in carrying out the lawful interception of communications. In the United States, the answer to this problem was the Communications Assistance for Law Enforcement Act (CALEA) in 1994.[3] The purpose of CALEA was to ensure that law enforcement surveillance capabilities remained 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 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 inter-

[3] 47 U.S.C. §§ 1001–1010 (2012).

cepted. Then, at the switch, the wiretap order could be implemented.

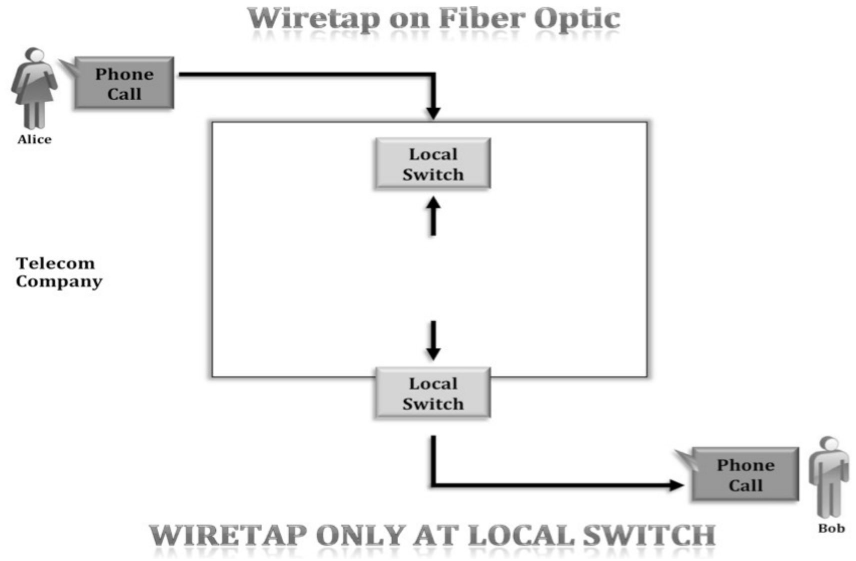

Figure 2. Fiber Optic Wiretapping

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, with a feed running from the switch to the agent's office. Along with these advantages for surveillance agencies, a clear limit was written into the statute. The legislative compromise at the core of CALEA provided that new wiretap ready requirements only applied to voice networks and did not apply to internet protocol communications.[4]

Coincidentally or not, the exponential growth of the Internet began just as CALEA was enacted. CALEA required telephone companies to submit new technologies to the FBI for review before they could be used. By contrast, new Internet software and hardware technologies proliferated as the estimated number of users grew at an incredible rate from 1994 to 2000, when the estimated number of Internet users exceeded 400 million people.[5] It is hard to imagine attaining this level of growth if software and hardware developers had been subject to the same FBI clearance requirements as their voice network counterparts.

[4] 47 U.S.C. § 1002(b)(2)(A) (2012) (excluding "information services").

[5] Central Intelligence Agency, The World Factbook 2001 (2001), *available at* http://www.umsl.edu/services/govdocs/wofact2001/geos/xx.html (estimating 407.1 million Internet users in 2000).

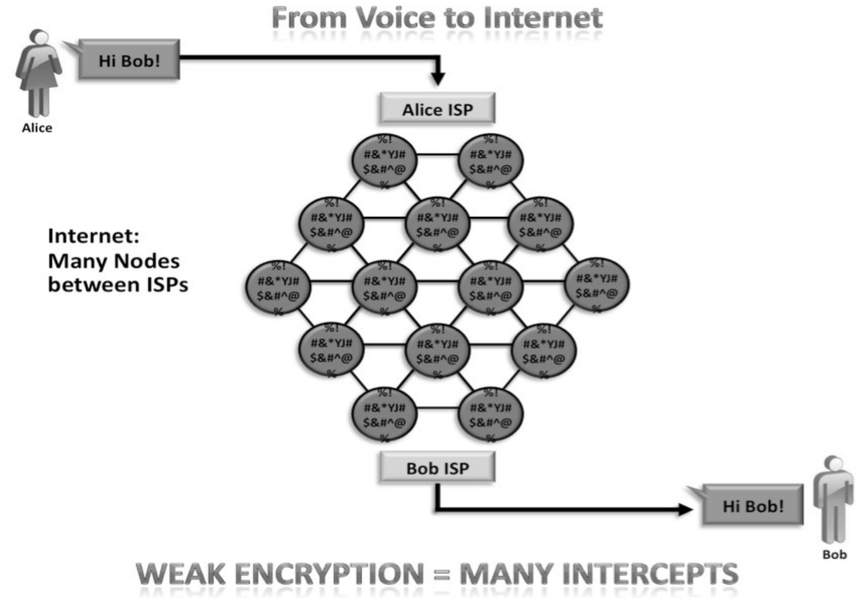

Figure 3. Internet Packet Routing

As the telephone networks complied with CALEA, the rapid growth of the Internet in the 1990s made the importance of strong encryption 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 to the networks. 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 termed this the "geodesic network" in which each node of the Internet is analogous to the nodes of the geodesic domes pioneered Buckminster Fuller.[6] Figure 4 provides an example of a geodesic dome. In a geodesic network, there are innumerable paths between any two points in a large network. If one route is blocked, the communication can simply travel through alternate nodes to arrive at its destination.[7]

[6] *See generally* Peter W. Huber, *The Geodesic Network: 1987 Report on Competition in the Telephone Industry* (1987) (discussing the geodesic network).

[7] Early Internet theorist John Gilmore popularized the concept that "[t]he Net interprets censorship as damage and routes around it." Philip Elmer-

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.

Figure 4. Geodesic Dome

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 companies, universities, and other organizations. However, there was no guarantee that communications would travel only 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

DeWitt, *First Nation in Cyberspace*, Time, Dec. 6, 1993, *available at* http://www.-time.com/time/magazine/article/0,9171,979768,00.html (quoting John Gilmore).

attack from outsiders who had taken control of the amateurs' computers. Additionally, nodes could be operated by hostile foreign governments or by entities reporting to such 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 third parties. Consider financial transactions that could be intercepted by criminals. These malicious parties could steal payments intended for others, or make copies of the transactions and attempt to cash in multiple times. Few would conduct serious business on the Internet if they believed that malicious parties would access and read their communications. Technical experts familiar with this vulnerability argued vehemently in favor of strong encryption so that personal communications and business transactions would be protected. As discussed below in Part III, technology industry leaders, civil right activists and technical experts alike quickly recognized the need for strong encryption on the Internet.

II. Encryption Concepts Relevant to the Legal and Policy Analysis

In order to understand the policy and legal issues discussed later in this Article, it is helpful to review some basic cryptographic concepts: private-key (or "symmetric") encryption; public-key (or "asymmetric") encryption; other cryptographic tools such as one-hashes and authentication; 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 for sending messages in a format that only intended recipients could read and understand.[8] 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 new and significant need for encryption due to the numerous intervening parties between the sender and recipient. The radio also encouraged the development of encryption,

[8] *See generally* David Kahn, The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet (1996) (providing a useful history of cryptology).

because both friends and enemies could listen to transmissions. One well-known example of radio encryption 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 consists of three major elements: (1) an encryption mechanism, typically a mathematical algorithm for turning plaintext (the original message) into ciphertext (the message in encrypted form); (2) a decryption mechanism, typically an algorithm for turning ciphertext back into plaintext; and (3) a mechanism for generating and distributing keys. A cryptographic key functions similarly to a physical key or combination lock. A physical key is cut slightly differently to fit a particular lock, such as for a car. Similarly, a combination lock, similar to those used for high school lockers, uses a sequence of numbers or symbols to open the lock.

To take a simple example, suppose that encryption occurs 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", or the number of 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 that situation, the key could range from the numbers 1 to 26.

In this approach, Alice and Bob would use the same encryption algorithms for encoding and decoding a message. When Alice wishes to send a message to Bob, she wraps the plaintext message with an agreed-upon secret key. Upon receipt of the encrypted message, Bob unwraps the message using the same private key. This approach is known as "symmetric" encryption, because the key is the same on both ends of the communication. It is also known as "private key encryption," because the key has to remain private—secret—to possible attackers, and known only to Alice and Bob.

The critical element in this approach is to generate and share the key securely. To distribute and share the symmetric keys, the Germans printed codebooks for each U-boat and other naval vessel. German officers were instructed to destroy the codebooks if faced with imminent capture. Eventually the Allies captured German codebooks revealing the keys used for particular dates.[9] Large

[9] John Barratt, *Enigma and Ultra: the Cypher War*, Military History Online (Dec. 15, 2002), http://www.militaryhistoryonline.com/wwii/atlantic/enigma.aspx.

portions of German communications became readable, greatly helping the war effort.[10]

B. Public Key or Asymmetric Encryption

A new and radical departure from traditional encryption methods developed during the 1970s and eventually became one of the most well known and widely used cryptosystems on the Internet. This "public key" or "asymmetric" encryption system was derived from the Diffie-Hellman multi-user encryption concept.[11] The first practical implementation of this cryptosystem became known as RSA, based on the names of cryptographers Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman.[12]

Instead of sharing the same key between Alice and Bob, asymmetric encryption uses different keys for encryption and decryption. 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 mathematics of an asymmetrical encryption algorithm are beyond the scope of this Article but the basic concept behind the public-key system is simple.[13] The process depends on a "one way function," a calculation that is much easier to execute in one direction than it is to reverse.[14]

[10] Some historians believe that these and other encryption discoveries may have shortened the length of World War II by two years or more. *See* Sir Harry Hinsley, Lecture at Cambridge University: The Influence of ULTRA in the Second World War (Oct. 19, 1993), *available at* http://www.cl.cam.ac.uk/research/security/Historical/hinsley.html.

[11] Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, IT-22 IEEE Transactions on Info. Theory 644 (1976).

[12] *See* Rivest et al., *supra* note 2.

[13] *See generally Standards Initiatives*, RSA.com http://www.rsa.com/rsalabs/node.asp?id=3122 (last visited Aug. 3, 2011) (providing information on the mathematical process of deriving public keys using the RSA algorithm).

[14] Bruce Schneier, *One-Way Hash Functions*, 16 Dr. Dobb's J. 148 (1991), *available at* http://drdobbs.com/database/184408620 (providing a useful explanation of a one-way function).

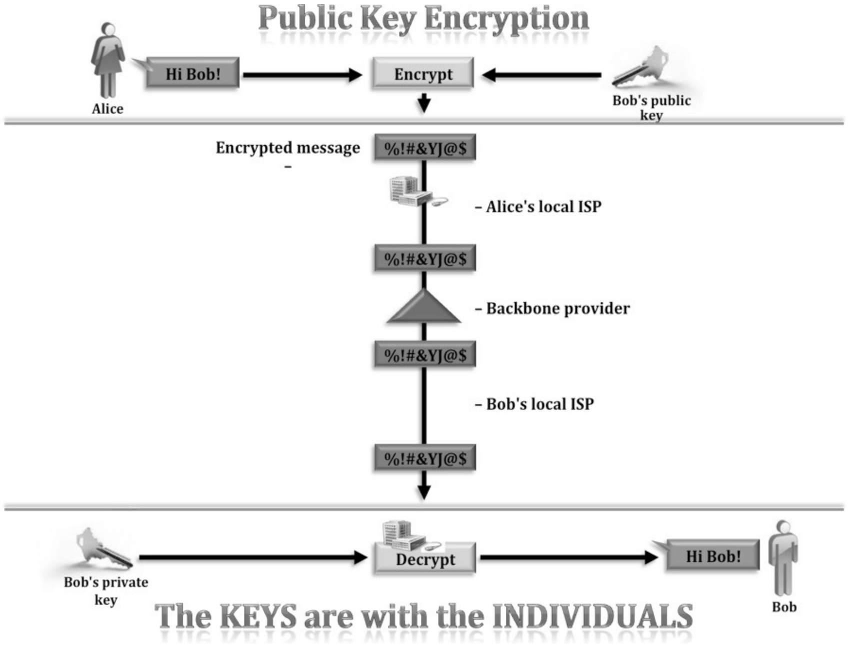

Figure 5. Public Key Encryption System

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 is a good fit for communication between geographically dispersed people on the Internet. It also addresses the traditional distrust for shared secrets among cryptographers, who often quote Benjamin Franklin's observation that "three may keep a secret, if two of them are dead."[15]

A second and related theme 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 this incremental user does not change the risk for existing users.

[15] Benjamin Franklin, Poor Richard's Almanac (1735).

C. Cryptographic Uses of Hashes and Authentication

The term "cryptography" (Greek for "hidden writings") applies to more than just encryption (Greek for "putting into hiding"). First, cryptography includes "one way hashes." The term "hash" conveys the image of a one-way operation—it is easy to turn an animal into the "hash" that people sometimes eat for breakfast; it is impossible to turn that hash back into a breathing cow or pig. Hashes are used widely in modern computing. One category of one-way hashes is a digital signature. Hashes travel with a message and mathematically ensure that the original message has not changed in transit—if even one letter is altered, the hash of that message will not match the hash of the original message.[16] Hashes can be strong or weak, and similar to encryption, a stronger hash is more difficult for an attacker to reverse.

Second, modern cryptography relies heavily on secure authentication to distinguish authorized from unauthorized users. One well-known example is the two-factor authentication 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.[17] 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 who uses an old key will be blocked from entry.[18]

D. Categories of Encryption Vulnerabilities

Although public-key encryption greatly helps key distribution, all forms of encryption are 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,

[16] *See* Rivest et al., *supra* note 2.

[17] In 2011, an embarrassing data breach at the RSA Security division of the EMC Corporation resulted in the apparent compromise of RSA's key fob encryption keys. The cryptosystem itself was apparently not compromised. *See* John Markhoff, *SecurID Company Suffers a Breach of Data Security*, N.Y. Times, Mar. 17, 2011, at B7 , *available at* http://www.nytimes.com/2011/03/18/technology/18secure.html.

[18] *See* *RSA Authentication Manager Express*, RSA.com, http://www.rsa.com/products/AMX/ds/11241_h9006-amx-ds-0711.pdf (last visited Apr. 18, 2012) (explaining how RSA's two-factor authentication system works).

or "backdoors." Understanding these categories of attacks is directly helpful to current policy debates about encryption.

1. Brute force attacks and the importance of key length

In a brute force attack, a hacker uses a computer program to attempt every possible combination of characters until one can read the plaintext. That is why key length is so important to the policy debates about encryption. The attacker can quickly exhaust every possible combination for a short key length, but may lack the computational power to break a long key.

With apologies to readers who do not like mathematics, the significance of key length is much easier understood through a review of a few basic exponent rules. Key length is measured in bits, where each digit is either zero or one.[19] A 10-bit key has 2 to the 10th combinations, or 1,024 possible keys. An 11-bit key doubles the number, to 2,048 possible keys. And 2 to the 12th doubles that number to 4,096 possible keys. This example illustrates how adding to the key length produces exponential growth in the number of possible key combinations. One might mistakenly think that increasing from 10 bits to 12 bits would make attacks 20% harder, because 12 is 20% higher than 10. That is incorrect. Instead, increasing from 10 bits to 12 bits makes the job 300% harder, from 1,024 possible key combinations to 4,096 possible combinations.

This basic concept of exponential growth is central to the logic behind brute force attacks. Current encryption law in India, written in 2000, limits key length to 40 bits.[20] This key length is trivially easy to break. By 1996, leading cryptography experts demonstrated that a 40-bit key could be broken in five hours at an equipment cost of $400.[21] 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 of 1,024 bits.[22]

[19] A "bit" is a term for binary digit, the basic unit of information used in computing.

[20] *See* Gov't of India, Ministry of Commc'n & IT, Dep't of Telecomm., Licence Agreement for Provision of Internet Services, cl. 2.1(vii), *available at* http://cca.ap.nic.in/i_agreement.pdf ("The Licensee shall ensure that Bulk Encryption is not deployed by ISPs. Further, Individuals/ Groups/ Organizations are permitted to use encryption up to 40 bit key length in the symmetric key algorithms or its equivalent in other algorithms without obtaining permission from the Licensor.").

[21] Matt Blaze et al., *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security* (Jan. 1996), *available at* http://www.schneier.com/paper-keylength.pdf.

[22] Banking Industry Tech. Secretariat et al., Email Sender Authentication Deployment: Best Practices and Considerations for Financial Institutions 44

Long key length is important in a cryptosystem, but by itself, does not guarantee that an encrypted message is secure. Flaws may exist in the implementation of the cryptosystem or the cryptosystem itself. As an analogy, imagine that an attacker is attempting to break into a room. A long key is akin to a steel door—it is very difficult to penetrate. A short key is similar to a paper door—it is easy to break through. A steel door is useful but will not keep attackers out if a window is open or the wall is made out of flimsy wood. Sufficiently long keys are thus necessary but only one element of a secure cryptosystem.

2. Improving brute force attacks and the importance of peer review

An important category of decryption work is improving the efficiency of brute force attacks. An ideal encryption system would make the likelihood of each possible key precisely the same. In that setting, an attacker would on average need to attempt half of the total number of possible combinations in order to chance upon the correct key.[23] Suppose, however, that the attacker somehow discovers that only even numbers are used in the keys and no odd numbers. For a long key, this would still leave the attacker with considerable work. Importantly, however, the number of possible combinations would be reduced by half, and the average time needed to discover the correct key would now be 25% of the time originally needed to test all of the combinations.[24]

Cryptographers generally agree that it is extraordinarily difficult to create an encryption algorithm that generates keys entirely randomly. Many algorithms proposed over time are flawed, as in the overly simplified example provided in the paragraph above. As a leading cryptography text states that:

(2009), *available at* http://www.bits.org/publications/security/BITSSender-AuthDeployJun09.pdf. Mathematically, a 1024-bit key length has 2^{984} more combinations than a 40-bit key length.

[23] The average number is half of the number of total combinations because occasionally the attacker will get lucky and the key will occur in the first 1% of combinations attempted. Occasionally the attacker will be very unlucky and the key will occur in the last 1% of combinations attempted. Those lucky and unlucky occasions have an average of (1+99)/2=50% of occurring. This simple example illustrates why random chance will lead to an average outcome of about 50% of the combinations.

[24] 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). Thus the average time to solve the key would be the time it takes to calculate ¼ of the total possible combinations.

> [t]here 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.[25]

Until a cryptosystem has withstood public scrutiny and rigorous peer review, it will endure considerable skepticism from experts. This has been a controversial issue in relation to China's encryption algorithms, which, as described below, were developed without public peer review. In addition, a strong cryptosystem and a long key length are not sufficient to ensure security—many vulnerabilities may arise at the implementation level, when the cryptosystem is actually deployed in a larger information technology system.

3. Backdoors

Another category of possible encryption system vulnerabilities occurs when a programmer intentionally creates the vulnerability. These security flaws are known as "backdoors." The image is that the front door to a house is securely locked, but someone can enter through a backdoor that appears to be locked, but is actually easy to open.

Intentionally creating backdoors can be attractive to some stakeholders. For instance, a system administrator might retain access to all data and communications in a system to ensure that organization policies are being followed.[26] More importantly, for wiretaps, CALEA requires the traditional telephone system to install a backdoor—to be designed wiretap accessible. Law enforcement and national security agencies have also sought back-

[25] Niels Ferguson et al., Cryptography Engineering: Design Principles and Practical Applications 13 (2010).

[26] In the U.S., employees who send emails over corporate network systems typically do not have a reasonable expectation of privacy in their communications. *See, e.g. McLaren v. Microsoft Corp.*, No. 05-97-00824-CV, slip. op. (Tex. App. May 28, 1999) (holding that employee had no reasonable expectation of privacy for emails stored in a password-protected folder on his employer's network system); *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 101 (E.D. Pa. 1996) (finding "no reasonable expectation of privacy in electronic communications voluntarily made by an employee to his supervisor over the company email system notwithstanding any assurances that such communications would not be intercepted by management"). In addition, the Electronic Communications Privacy Act, which authorizes criminal sanctions for those who intentionally access e-mail services without authorization, contains an exception providing that employers may access their own private network systems with full authority. Electronic Communications Privacy Act of 1986, 18 U.S.C. 2511(2)(a)(i) (1986).

doors for encrypted communications, such as through the "key escrow" approach discussed below.

The main problem with backdoors, however, is that it is extremely difficult to install a backdoor that can be used by the "good guys," such as authorized law enforcement wire tappers, but not by the "bad guys." In one widely publicized incident in Greece, intruders gained access to the interception capabilities designed for use by law enforcement. The phone calls of the Prime Minister and over one hundred other high-ranking government officials were illegally wiretapped, and the perpetrators were never caught.[27] The risks of using backdoors are a main theme of cryptography expert Susan Landau's recent book entitled, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*.[28] As Landau documents, backdoors intended to facilitate government surveillance can pose security problems that exceed the benefits received from the information collected.

III. FROM THE U.S. "CRYPTO WARS" TO THE NEW GLOBAL ENCRYPTION DEBATES

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

A. The Crypto Wars

Prior to the 1990s, the National Security Agency (NSA) played a dominant role in U.S. cryptography. As an agency in 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, decrypting codes used by foreign forces or other targets of communications surveillance. The second role was defensive—protecting the use of effective encryption by the U.S. military, the rest of the U.S. government, and key industries. After World War II and until the development of public key encryption, the NSA regularly recruited many of the country's best

[27] Vassilis Prevelakis & Diomidis Spinellis, *The Athens Affair*, IEEE Spectrum (July, 2007), *available at* http://spectrum.ieee.org/telecom/security/the-athens-affair.

[28] *See* Susan Landau, Surveillance or Security? The Risks Posed by New Wiretapping Technologies 175–202 (2011).

cryptographers.[29] The NSA's dominant role diminished as computer technology advanced and public key cryptography developed in public, rather than being classified as a national security secret. 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. The NSA in particular made numerous attempts to stifle the outside development of encryption.[30] By the end of the George H.W. Bush administration in 1992, non-NSA encryption had become an important issue for national security policymakers.[31]

1. Key escrow and the "Clipper Chip"

When President Clinton entered office, the concepts of "key escrow" and "Clipper chip" became the central battleground for debates about encryption.[32] For the administration, key escrow appeared to provide a way of allowing strong encryption for ordinary communications while still enabling access when needed to law enforcement and national security agencies. With key escrow, the government would permit the widespread use of strong cryptosystems and sufficiently long keys to protect communications against brute force attacks. The tradeoff, however, was that users of strong encryption would be required to store their keys with the government—the keys would be held in "escrow."[33] The govern-

[29] Between 1949 and 1960 the NSA's staff of cryptographers increased from 4,139 to 12,120. Thomas R. Johnson, American Cryptology during the Cold War, 1945-1989, at 64 (Center for Cryptologic History, National Security Agency 1995), *available at* http://www.nsa.gov/public_info/_files/cryptologic_histories/cold_war_i.pdf. The recruitment of talented young cryptographers is prominently featured in two popular movies. In A Beautiful Mind (Universal Studios 2001) actor Russell Crowe played the role of real-life mathematician John Nash who was hired by the government to work on cryptography. Similarly, in Good Will Hunting (Miramax Films 1997) the fictional Will Hunting, played by Matt Damon, was recruited to use his cryptographic talents for the government, but refused employment.

[30] This included the use of secrecy orders against researchers and the revocation of funding for outside cryptography research. *See* Steven Levy, Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age (2001).

[31] *Id.*

[32] In addition to the detailed history provided in the Levy book *supra* note 30, helpful resources on the U.S. encryption controversy are available from the relevant public interest groups. *See Cryptography*, Center for Democracy and Technology, http://www.cdt.org/crypto (last visited Aug. 15, 2011). *See also Cryptography Policy*, Electronic Privacy Information Center, http://epic.org/crypto (last visited Aug. 15, 2011).

[33] 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

ment planned to establish two separate key-escrow data banks, to be run by independent entities, each of which would hold one part of the key.[34] Upon proof of a proper court order for a suspect's communications, the two key-escrow data banks would reveal their parts of the key to the agency.[35] That agency could then use the two parts of the key together to decipher the encrypted communications and read them in plain text. Unrelated communications would remain strongly encrypted and unavailable to the government agencies.

The Clipper chip was the government's first attempt at implementing a key escrow system. The basic concept was that a chipset would be installed in all new voice communication devices, each of which would be designated an encryption key. Each half of the key would be escrowed with a different and separate entity. Through proper legal process, law enforcement and national security agencies could retrieve the escrowed keys and access the plaintext 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. The term "Clipper chip" soon became shorthand for referring to a much broader policy debate about government controls on encryption.

The Clipper chip was never launched on a meaningful scale, as manufacturers failed to warm to the controversial government-designed chip. Also, in 1994, cryptographer Matt Blaze discovered ways in which the Chip's implementation was technically flawed, so that the escrowed key would not decipher phone communications.[36] Perhaps most importantly, the proposal incited impassioned opposition to government controls on encryption, especially from leading civil liberties groups and "techies"[37]—a vocal constituency who were in the midst of creating the revolution

fulfillment of a condition." *Definition of Escrow,* Merriam-Webster, http://www.merriam-webster.com/dictionary/escrow (last visited Aug. 7, 2011). Applied to encryption, the key would be the property held in trust by an escrow authority established by the U.S. government. The key would be turned over to law enforcement or national security agencies when legal conditions were fulfilled.

[34] Statement by the Press Secretary, Office of the Press Secretary, The White House, The Clipper Chip Initiative (Apr. 16, 1993), *available at* http://epic.org/crypto/clipper/white_house_statement_4_93.html.

[35] 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 key would only be revealed if two separate data banks were accessed, and collusion between the two data banks would be difficult.

[36] Matt Blaze, *Protocol Failure in the Escrowed Encryption Standard*, Proceedings of the 2nd ACM Conference on Computer and Communications Security 59-67 (ACM Press, 1994), *available at* http://www.crypto.com/papers/eesproto.pdf.

that was growing the Internet from its first commercial activities in 1993 to over 390 million users by 2000.[38] For a flavor of the opposition to encryption controls, consider the 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."[39]

2. Critiques of key escrow and their current relevancy

Key escrow persisted as a government policy even after the failure of the Clipper chip, prompting encryption experts to publish a comprehensive critique of key escrow in 1997.[40] Because the value of key escrow continues to be debated today (currently in India), it is useful to highlight three dimensions of the critique. First, key escrow increases the security risks in operating an encryption system. As with any backdoor, the system is rendered vulnerable to attacks related to the backdoor. In particular, the storage of the keys in a central database creates "high-value targets for criminals or other attackers."[41] In addition to potential abuse by database insiders, communications to and from the key escrow recovery center become a prime target for attack. For instance, one proposed approach involved keys being 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."[42]

[37] 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. *See Archived CPSR Resources on Privacy*, Computer Professionals for Social Responsibility, http://cpsr.org/prevsite/program/privacy/privacy.html/ (last updated April 22, 2003).

[38] *See* http://data.worldbank.org/indicator/IT.NET.USER?page=2 (World Bank data showing number of internet users worldwide in 2000).

[39] John Perry Barlow, *Decrypting the Puzzle Palace*, 35 Comm. of the ACM Vol. 35, No. 7 (July 1992) at 25, 29, *available at* http://dl.acm.org/citation.cfm?id=129910&bnc=1.

[40] The key escrow critique was drafted and signed by a veritable "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. Hal Abelson et al., The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption (1997), *available at* http://www.schneier.com/paper-key-escrow.pdf.

[41] *Id.* at 11.

[42] *Id*. at 18.

Second, the experts emphasized the inherent difficulty of building and operating a key escrow system. Complexity is a major challenge in developing and implementing any encryption system. A key recovery system greatly multiplies this complexity, especially given the desire of law enforcement and national security agencies to access communications within hours of transmittance, or even less. The experts asked readers to consider the complexity of these steps:

> [R]eliably 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; 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.[43]

Each step is subject to possible attacks, such as through presentation of false law enforcement credentials or court orders. Because so many parties interact, it is enormously complicated to enable law enforcement access (the "good guys"), while rigorously excluding unauthorized access (the "bad guys").

Third, there are high costs associated with creating and maintaining such a complex key escrow system. These costs include: the overhead of operating the system; product design and testing costs, which must be rigorous and extensive to assure the highest level of security consistent with key escrow; and costs for all users who are required by law to comply with key escrow requirements. This also includes the potentially irreparable costs to users in the likely event that their communications are compromised. In the face of such a comprehensive critique, any plan to implement a key escrow system should thoroughly consider the many potential vulnerabilities and costs inherent in this approach.

3. Export controls and proposed limits on domestic encryption

After the failure of the Clipper chip, the Clinton Administration continued to explore regulatory means through which it could control the use and development of encryption. Public debates about these issues focused primarily on government-imposed export controls and secondarily on proposals limiting use of encryption within the U.S.

[43] *Id.* at 15.

For those unfamiliar with encryption, it may seem odd that encryption software was historically classified as a "munition," and thus subject to the same export controls that applied to advanced military technologies such as fighter jets.[44] The history of Enigma in World War II, however, illustrates the military importance of breaking enemy codes and ensuring the security of sensitive communications.

The precise elements of the U.S. encryption export regime shifted during the 1990s, with the Commerce, State, and other departments playing different and varying roles. By the mid-1990s, export of even moderately strong encryption required a license from the Department of Commerce. Companies that pushed the envelope on encryption export faced the risk of denial and the inability to sell their goods overseas. The government would also periodically issue broad regulations affecting the export of encryption. A 1996 regulation, for instance, stated: "The plan envisions a worldwide key management infrastructure with the use of key escrow and key recovery encryption items."[45]

The export control regime meant that major information technology companies were constantly engaged in difficult negotiations with the federal government, especially because products were evolving so rapidly during this period of intense Internet growth. Export limits were particularly burdensome for the many IT companies that conducted substantial business overseas. Those companies faced the difficult choice of either selling weak encryption products in all markets, or else establishing two tiers of products, one for the U.S. market and one for export abroad. Over time, the export rules 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. export control rules. A growing concern was thus that strong encryption was in fact being deployed outside of the U.S., but the export controls were preventing U.S. companies from meeting that demand.

The stakes were raised 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

[44] *See* U.S. Congress, Office of Tech. Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606 (1994), 151 (describing how cryptography was classified under the Arms Export Contol Act and International Traffic in Arms Regulations).

[45] Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68572 (Dec. 30, 1996) (to be codified at 15 C.F.R. pts. 730, 732, 736, 738, 740, 742, 744, 748, 750, 768, 772, and 774).

U.S. had permitted research and use of strong encryption within the country. Limiting the strength of domestic encryption, however, 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 deployed in the U.S. would likely spread abroad over time, despite export rules. Proposed limits on domestic encryption, however, lifted 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 the proposed limits on domestic encryption, analogous to the technical critique of key escrow discussed above.[46] As the crypto wars raged on, the proposal to limit domestic encryption was blocked in Congress. Free speech based objections to encryption limits met with some success in federal court.[47] Meanwhile, the public-key encryption program called PGP (Pretty Good Privacy) became widely available on the Internet.[48] As this PGP software spread, attempts to prevent use of strong encryption became increasingly futile. Once PGP could be easily downloaded from anywhere in the world, members of Congress and others increasingly realized that the controls should be lifted.[49]

4. The 1999 shift in administration policy

In September 1999, the Clinton administration shifted its position on encryption policy and announced that it would lift most export controls on encryption. Secretary of Commerce Daley said:

[46] The critique was first drafted by Michael Froomkin, Lawrence Lessig, and Peter Swire, then signed by thirty law professors and sent as an open letter to the House Commerce Committee. Letter from Keith Aoki et al., to The Honorable Thomas J. Bliley (Sept. 23, 1997), *available at* http://www.cdt.org/crypto/legis_105/SAFE/97093_profs.html.

[47] *See Bernstein v. U.S. Dep't of Justice*, 945 F. Supp. 1279 (N.D. Cal. 1996). College professor Daniel Bernstein 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.

[48] PGP is an encryption program created by cryptographer Phil Zimmermann in 1991. *See generally* Philip R. Zimmermann, *Why I Wrote PGP*, Philip Zimmermann (June 1991), http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html (explaining Zimmermann's PGP creation and public release).

[49] In 1999, there were over 200 co-sponsors of a bill to lift encryption export controls known as the Security and Freedom through Encryption (SAFE) Act H.R. 850, 106th Cong. (1999).

"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."[50] 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."[51] The administration explicitly endorsed the view that strong encryption is needed for the Internet. Peter Swire, the administration's Chief Counselor for Privacy, said:

> Today'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.[52]

The 1999 announcement decisively changed U.S. law and policy on encryption and effectively brought the crypto wars to an end. The key factors that led to this result are subject to debate. Politics certainly played a role, including effective advocacy by IT companies and privacy groups, as well as Vice President Gore's desire to win the support of these groups as he headed into the 2000 presidential election. Members of both parties in Congress became increasingly opposed to the old administration position, based on the view that American companies would otherwise lose market share and that strong encryption would inevitably become widely available from other countries.

Swire's view is that the merits of strong cryptography were fundamental in the eventual shift in policy. Any government is inclined to listen closely to law enforcement and national security advisors when they warn against problems caused by new technology. Over time, however, two basic conclusions became clear: (1) strong cryptography is essential to the growth and success of an open network such as the Internet; and (2) no technical fix, such as

[50] 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), *available at* http://www.epic.org/crypto/legislation/cesa/briefing.html [hereinafter Press Briefing].

[51] Statement by Commerce Secretary William Daley Re: Administration encryption policy (Sept. 16, 1999), *available at* http://www.techlawjournal.com/cong106/encrypt/19990916dal.htm.

[52] Press Briefing, *supra* note 50 (Statement of Peter Swire).

key escrow, was available to provide access only to the "good guys" but not the "bad guys." In the White House announcement on encryption policy, then Deputy Secretary of Defense Hamre echoed these conclusions:

> We in the Defense Department [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.[53]

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

Encryption policy developments in India and China are noteworthy not only because of the countries' 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 standard used in these major markets and populations, then the cybersecurity of the Internet will be severely weakened. Many of the issues these countries are grappling with today were debated during the U.S. crypto wars of the 1990s. Accordingly, it is important keep in mind the lessons learned in the 1990s when examining the emerging encryption debates, in India, China, and elsewhere globally.

1. India

India's current encryption policy is best understood as a response to the 2008 Mumbai bombings, which left more than 170

[53] *Id.* (Statement of John Hamre). In Swire's view, the DoD's changing position on encryption controls was central to the administration's eventual shift in policy. Initially, the NSA's surveillance concerns dominated over other agencies, and the DoD strongly supported its limits on encryption. Over time, however, the DoD realized its own dependence on the Internet and need for effective encryption. In addition, the DoD (primarily the FBI and DOJ) wished to retain world-class encryption expertise within the United States, and did not want its strong encryption to be supplied by foreign nations. This position attracted increasing support, ultimately isolating the NSA in interagency debates, and eventually leading to the 1999 change in administration policy.

dead and hundreds more injured.[54] Responsibility for the attacks has been attributed to terrorist groups allegedly funded by Pakistan.[55] In the aftermath of the attacks, the Government of India and its security agencies launched an ambitious plan to increase their lawful intercept capabilities. In 2010, a highly publicized dispute with Research in Motion (RIM), the manufacturer of Blackberry, centered on India's demand for the encryption keys to messages transmitted over the Blackberry Enterprise Server.[56] Development of a uniform national encryption policy has thus become a controversial issue in New Delhi.

In India, 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 Telecommunications, developed in the late 1990s, 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.[58] It also restricts end users from using encryption, or systems (e.g. Blackberry) providing encryption, with greater than a 40-bit key length.[59] Up until the 2008 Mumbai bombings, these rules were not widely enforced. Indian individuals and corporations regularly used 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, financial agencies must use keys of at least 128-bit length to comply with recommendations issued by the Securities and Exchange Board of India.[60] These varying standards have

[54] *See Mumbai Attacks*, BBC News (last updated Oct. 18, 2010, 13:14 UK), http://news.bbc.co.uk/2/hi/in_depth/south_asia/2008/mumbai_attacks/default.stm (providing links to articles and timelines of the 2008 Mumbai bombings).

[55] *See Four Pakistanis Charged by US Over 2008 Mumbai Attacks*, BBC News (Apr. 26, 2011), http://www.bbc.co.uk/news/world-south-asia-13194861.

[56] Vikas Bajaj, *India May Be Near Resolution of BlackBerry Dispute*, N.Y. Times, Aug. 18, 2010, at B4, *available at* http://www.nytimes.com/2010/08/18/business/global/18rim.html.

[57] *See Internet Without Telephony*, Dep't of Telecomm., Ministry of Commn'n & Info. Tech. of the Gov't of India, http://www.dot.gov.in/isp/ispindex.htm (last visited Aug. 15, 2011). *See also Internet With Telephony*, Dep't of Telecomm., Ministry of Commn'n & Info. Tech. of the Gov't of India, http://www.dot.gov.in/ispt/isptindex.htm (last visited Aug. 15, 2011).

[58] *Guidelines and General Information for Grant of License for Operating Internet Services*, Dep't. of Telecomm., (Aug. 24, 2007) at 8, *available at* www.dot.gov.in/isp/Internet%20Service%20Guideline%2024-08-07.doc.

[59] *Id.*

[60] *Master Circular For Stock Exchanges on Trading Part-II*, Sec. and Exch. Bd. of India, (Oct. 11, 2000), *available at* www.sebi.gov.in/circulars/2010/anncir2.pdf.

prompted calls for a modern and uniform national encryption system. The Information Technology Act of 2008 permits the government to develop a new encryption policy, independent of telecom licensing guidelines.[61]

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. The Information Technology Act of 2008 provides that the government can intercept, monitor, or decrypt any electronic data for national security purposes.[62] The government can also order the lawful interception of communications under the Indian Telegraph Act of 1885, with a written order.[63]

For business customers who have used the Blackberry Enterprise System, RIM and other providers repeatedly stated that it does not have the ability to turn over the decryption keys to the government because only the enterprise users possess them. RIM's position is consistent with the authors' own understanding of how the Blackberry Enterprise System operates.[64] In response, the government threatened to shut down providers who do not comply with the strict legal limits on encryption, including the 40-bit limit on key length. In early 2012, RIM agreed to set up a server in Mumbai, with lawful access available to Indian agencies. With this server, Indian agencies will be able to access individual Blackberry accounts, but the Indian government eventually decided that Blackberry Enterprise System accounts are not of "high concern," and access will not be provided to the plaintext of those communications.[65]

The current encryption controversy in India has important similarities with the U.S. crypto wars of the 1990s. Indian national security and law enforcement agencies are encountering technical obstacles to their wiretaps, involving the use of encryption. These

[61] The Information Technology (Amendment) Act, No. 10 of 2008, Acts of Parliament, 2009 (India), *available at* http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf [hereinafter IT Act of 2000 (as amended)].

[62] *Id.* at 12 (IT Act of 2000 (as amended) Section 69).

[63] The Indian Telegraph Act, No. 13 of 1885, India Code (1993), *available at* http://indiacode.nic.in (amended 2006).

[64] *See generally* BlackBerry Enterprise Server 5.0, Security Technical Overview 5.03 (Sep. 12, 2011), *available at* http://docs.blackberry.com/25762 (discussing how the BES encryption system operates).

[65] *RIM set up server for Indian govt. to intercept BBM data in real-time*, Thinkdigit, Feb. 21, 2012, http://www.thinkdigit.com/Mobiles-PDAs/RIM-sets-up-server-for-Indian-govt_8807.html. Nokia also agreed to establish a server in India. *Id.*

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 that effective cryptography is essential to modern computing. Another category of opposition comes from domestic Indian industries, especially the BPO (business process outsourcing) industry. The BPO sector risks losing business foreign competitors 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 U.S. Clipper chip proposal from the 1990s.[66] In early 2012, there were press reports that the Indian government would propose a law requiring companies that offer encrypted communications services to have part of their information technology infrastructure inside of India, to facilitate lawful access.[67] As was true in the United States, key escrow may initially seem attractive because it appears to simultaneously allow strong encryption for ordinary communications while also providing lawful access in the small subset of cases where there is a lawful intercept. Other sections of this Article detail the many technical and policy objections to this key escrow approach.

The future of India's encryption policy is difficult to predict. The argument in favor of bolstering national security is treated very seriously in India, which has ongoing tension with its nuclear-armed neighbor, Pakistan. There has been some discussion about imposing import controls on encryption so that importers would be required to obtain licenses in order to bring encrypted products and services into the country.[68] Meanwhile, as discussed in this Article, there are significant cybersecurity, business, and other objections to the legal limits on effective encryption that India is considering expanding.

2. China

China's approach to gaining traction in the global encryption market has differed greatly from international best practices that promote open, peer review for encryption standards. Rather than encouraging private sector development of encryption, China

[66] Interviews with Government of India officials were conducted by Peter P. Swire in March 2011 [hereinafter Swire Interviews].

[67] *See, e.g.,* Sahil Makkar & Shauvik Ghosh, *Govt plans rule for encrypted data access,* livemint.com, Jan. 12, 2012, http://www.livemint.com/2012/01/12001457/Govt-plans-rule-for-encrypted.html

[68] *Id.*

treats encryption as a national policy, subject to government direction and authority. All entities engaged in the domestic import, development, or sale of encryption products are subject to strict import and export licensing requirements.

These and other encryption regulations are bolstered by China's aggressive promotion of "Indigenous Innovation," a government policy that China hopes will launch itself to the forefront of the global technology market. The policy *fosters domestic technological development while limiting dependence on foreign technology.*[69] In 2006, China revealed its "National Medium and Long-Term Plan for the Development of Science and Technology (2006–2020)" in which it acknowledged that "despite the size of [its] economy, [China] is not an economic power, primarily because of weak innovative capacity."[70] One element of China's push for indigenous innovation involves gaining expertise in the areas of cybersecurity and encryption. In pursuit of this goal, China has placed limits on the use of international encryption standards by implementing a strict licensing regime and by mandating the use of domestic encryption algorithms that have not undergone public peer review.

a. China's import and export licensing regime

In 1999, the Chinese State Council issued the Administration of Commercial Encryption

Regulations, which established what is now known as the State Encryption Management Bureau (SEMB) to regulate the import, development, and sale of commercial encryption in China.[71] The Encryption Regulations effectively outlawed the use and sale of foreign products containing commercial encryption in China.[72] Specifically, the regulations required SEMB approval to research, develop, produce, distribute, and use commercial encryption products in China, as well as for the manufacture or distribution of commercial encryption products containing Chinese-developed

[69] *See generally* U.S. Chamber of Commerce, *China's Drive for "Indigenous Innovation": A Web of Industrial Policies* (2010), *available at* http://www.uschamber.-com/sites/default/files/reports/100728chinareport_0.pdf (analyzing China's Indigenous Innovation Policy of increasing domestic innovation and replacing foreign intellectual property with domestic intellectual property where possible).

[70] State Council PRC, Information Office, *The National Medium- and Long-Term Program for Science and Technology Development (2006–2020): An Outline*, (2006), *available at* http://www.cstec.org/uploads/files/National%20Outline%20for%20Medium%20and%20Long%20Term%20S&T%20Development.doc.

[71] Anne S.Y. Cheung, *The Business of Governance: China's Legislation on Content Regulation in Cyberspace*, 38 N.Y.U. J. Int'l L. & Pol. 1, 14–15 (2006).

[72] *Id.*

encryption technology.[73] They also prohibited the sale of encryption products produced by foreign countries without a permit. [74]

These new regulations created significant objections from foreign nations and companies about the ability of non-Chinese companies to compete in the Chinese market.[75] In response, the SEMB issued a new memorandum in 2000, stating that only hardware and software for which encryption and decoding operations are "core functions" were subject to the 1999 regulations. Other hardware and software (such as wireless telephones, Windows software, and Internet browser software), for which encryption was not the core function, would not be covered. [76] China did not specify standards for determining whether a device uses encryption as its core function. This lack of guidance has created great uncertainty among companies that wish to conduct business in China but rely on hardware, software, or services that deploy encryption.

b. China's certification and other security requirements

In 2007, China announced a mandatory domestic security certification system known as Chinese Compulsory Certification (CCC), for 13 categories of information security products. This certification must be obtained from China's Office of Security Commercial Code Administration (OSCCA) before the products can be used, produced, and marketed in China. The CCC is based on Chinese security standards, not international security technology standards. The certification process involves disclosure of the products' encryption source code, among other trade secrets, and appears to require the products to incorporate Chinese proprietary encryption algorithms. In the face of opposition from varying countries and technology industry alliances, China limited the certification requirements to products eligible for government procurement. Further efforts were undertaken to ensure that the broader category of State Owned Enterprises was not included in the definition of government procurement. This clarification was successfully obtained in 2009, although it is notable that government procurement still affects a wide range of commercial activities.

Separate from the certification system, in June 2007 China established guidelines regulating products integrated in critical infrastructure information systems. This Multi-Level Protection Scheme (MLPS) is very broad in scope and actually extends beyond "critical infrastructure" information systems to cover all

[73] *Id.*

[74] *Id.* at 15.

[75] *Id.* at 36.

[76] *Id.*

end-users.[77] MLPS specifies five levels of information systems, detailing technical standards for encryption and other security products used at each level.[78] Enforcement procedures related to the MLPS encryption requirements allow authorized enforcement agencies to "exercise complete control" over encryption used in MLPS systems, "access key management and other cryptographic protocols," and requires "that a significant portion of cryptographic source code" be turned over.[79]

c. Homegrown Encryption

As part of its indigenous innovation policy, China employs a strategy of developing proprietary national standards for encryption, which it has not traditionally made available for public review. The government provides local Chinese companies access to the algorithms for the purpose of complying with government regulations.

China's trusted computing module (TCM) is a prominent example of how Chinese encryption policy acts as a barrier to compliance with global standards. TCM is modeled on the Trusted Platform Module, a widely deployed chip with accompanying software that is intended to secure the proper functioning of an IT system. The TCM, however, requires use of Chinese algorithms, which were previously unavailable to the public. It also requires conformance with TCM specifications, which until recently were only available to domestic Chinese companies. These policies effectively shut the global TPM standard out of China's domestic market. Further, China uses commercial encryption regulations as the rationale for prohibiting the import of platforms that employ TPMs into China. In April 2011, China published nine trusted computing standards related to TCMs.[80] International experts are currently reviewing these standards and implementation documentation to determine completeness and feasibility of implementation. However, competing standards such as TCM are likely to continue to encounter interoperability and implementation challenges, and are also likely to have less thorough peer review globally, with its accompanying security advantages.

[77] Dieter Ernst, Indigenous Innovation and Globalization: The Challenge for China's Standardization Strategy 34 (2011), *available at* http://www.eastwestcenter.org/sites/default/files/private/ernstindigenousinnovation.pdf.

[78] *Id.*

[79] *Id.* at 35.

[80] *Trusted Computing*, U.S. Info. Tech. Office, http://www.usito.org/dev/policy-work/cybersecurity/trusted-computing (last visited Aug. 24, 2011).

Another example of homegrown encryption is China's wireless networking standard, the Wireless Authentication and Privacy Infrastructure (WAPI). WAPI was purportedly designed to resolve security flaws in Wi-Fi, the global standard for wireless networking.[81] In late 2003, China mandated the use of WAPI in all Wi-Fi systems sold and used in China.[82] This required all foreign wireless companies operating or manufacturing in China to partner with one of the few Chinese companies that possessed the WAPI encryption standard because the standard was not released to the public.[83] In 2006, the International Standardization Organization (ISO) rejected WAPI as an international standard.[84] The rejection was based in part on WAPI's use of an undisclosed encryption algorithm, hindering ISO's ability to effectively assess its security and completeness.[85] WAPI was resubmitted to ISO for approval in 2009.[86] After significant trade disputes between the U.S. and other countries about potential trade barriers, China decided not to make WAPI a mandatory standard.[87]

More recently, China has taken somewhat greater steps to engage with global standards for encryption. The ZuC algorithms, for use with LTE (Long Term Evolution) mobile communications, were designed by the Data Assurance and Communication Security Research Center of the Chinese Academy of Science.[88] Three ZuC algorithms were submitted for public evaluation to ETSI, an official European Standards Organization of the European Union.[89] The public evaluation of ZuC identified several flaws in the algorithms, and revised versions have been produced.[90] The ZuC algorithms were accepted by ETSI as an "optional" algorithm, meaning that use of the ZuC algorithms is consistent with

[81] *China: Intellectual Property Infringement, Indigenous Innovation Policies, and Frameworks for Measuring the Effects on the U.S. Economy*, U.S. Int'l. Trade Comm'n (Nov. 2010) at 5-15 to 5-16, http://www.usitc.gov/publications/332/pub4199.pdf [hereinafter *China: Intellectual Property Infringement*].

[82] *Id.*

[83] Ellen Messmer, *Encryption Restrictions*, Network World (Mar. 15, 2004, 10:05 PM), http://www.networkworld.com/careers/2004/0315man.html?page=1.

[84] *China: Intellectual Property Infringement*, *supra* note 81.

[85] *Id.*

[86] *Id.*

[87] *Id.*

[88] China Communications Standard Association, *ZUC Algorithms for Public Evaluation* (Sept. 15, 2010), http://www.ccsa.org.cn/english/zuc.htm.

[89] *Id.* For information on ETSI, see www.etsi.org.

[90] International Association for Cryptologic Research, *Mobile Phone Security Algorithms – New Version* (2012), http://www.iacr.org/news/2011-02-28_4GLongTermEvolution.html (last visited April 11, 2012).

the ETSI LTE standard. This step should be seen as welcome participation by the Chinese in global standards processes. Less welcome, however, are reports that China is treating use of ZuC as mandatory within China, which would mean that LTE equipment that complies with the LTE standard but lacks ZuC would be in violation of Chinese standards.[91]

3. Encryption in the rest of the world

India and China are not the only countries where encryption products are restricted. Among other countries, Russia also restricts the importation of products that contain encryption other than the Russian proprietary block cipher GOST. Recently, Russia failed to obtain international recognition of its GOST algorithm by the ISO because of known attacks on the algorithm.[92] The Russian government allows for the import of products containing encryption only through notification and licensing procedures. *Russia has also placed limits on the shipment of TPM platforms into Russia.*[93]

IV. WHY GLOBALIZATION STRENGTHENS THE CASE FOR ENCRYPTION

The crypto wars of the 1990s led to widespread awareness of the importance of encryption to computing and communications, especially for an insecure channel such as the Internet. This Part examines how the passage of time and the continued process of globalization further strengthen the case for strong encryption for two main reasons. First, encryption plays a central role in cybersecurity today. Encryption is now integral to the routine functioning of modern computing, far more so than when U.S. policy shifted in 1999. In cybersecurity today, attackers possess major advantages over defenders. Encryption is quite possibly the single most important tool for defenders, and it is thus vital to cybersecurity. Second is what we call "the least trusted country problem." If there are backdoors or limits on effective encryption, then the security of the global system is only as strong as the security in the least trusted

[91] Claire Vishik, *National, Regional, and International Standardization in Security* (Jan. 2012), http://workshop.etsi.org/2012/201201_SECURITYWORKSHOP/3_INTERNATIONAL_STANDARDIZATION/INTEL_VISHIK.pdf.

[92] *See* Ewan Fleischmann et al., *Key Recovery Attack on full GOST Block Cipher with Zero Time and Memory*, ISO Standard ISO/IEC JTC 1/SC 27 N8229 (2009) (summarizing known attacks on the GOST cipher). *See also* Nicolas T. Courtois & Michal Misztal, Differential Cryptanalysis of GOST, http://eprint.iacr.org/2011/312.pdf (last updated July 2, 2011).

[93] *See* Hewlett Packard, HP Trusted Platform Module, *available at* http://h18004.www1.hp.com/products/servers/proliantstorage/questionsanswers.html.

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 reports of cybersecurity threats and breaches become more prevalent, the need for strong encryption is more important than ever before.

1. The surprisingly recent rise of the cybersecurity issue

Today, there is widespread consensus on the importance and challenges of cybersecurity. In the United States, Congress, the President, the military, and civilian government agencies have all advanced varying proposals addressing cyber security.[94] Sentiment is similar in other countries around the world. For instance, public statements concerning cybersecurity by government leaders in India and the European Union sound quite similar to those by U.S. officials.[95]

The advent of cybersecurity as a leading policy matter is more recent than most would suspect.[96] The cybersecurity issue received

[94] *See* Press Release, Senate Homeland Sec. & Gov't Affairs Comm., Lieberman, Collins, Carper Unveil Major Cybersecurity Bill to Modernize, Strengthen, and Coordinate Cyber Defenses (June 10, 2010), *available at* http://lieberman.senate.gov/index.cfm/news-events/news/2010/6/lieberman-collins-carper-unveil-major-cybersecurity-bill-to-modernize-strengthen-and-coordinate-cyber-defenses; White House Fact Sheet: Cybersecurity Legislative Proposal (May 12, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal; Press Release, Speaker of the House of Representatives, Speaker Boehner & Leader Cantor Announce New Cybersecurity Task Force Led by Rep. Thornberry (June 24, 2011), *available at* http://www.speaker.gov/News/DocumentSingle.aspx?DocumentID=248724; Dep't of Defense Strategy for Operating in Cyberspace (July, 2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf; Dep't of Commerce, Cybersecurity, Innovation and the Internet Economy (June, 2011), *available at* http://www.commerce.gov/sites/default/files/documents/2011/june/cybersecurity_green_paper_finalversion_0.pdf.

[95] *See, e.g.,* Indo-Asian News Service, *India Faces Security Threat from Cyber World*, Thaindian.com (Feb. 2, 2011), http://www.thaindian.com/newsportal/sci-tech/india-faces-new-security-threat-from-cyber-world_100501409.html; Warwick Ashford, *Cyber attacks and terrorism top security strategy priority list*, ComputerWeekly.com (Oct. 10, 2010), http://www.computerweekly.com/Articles/2010/10/18/243387/Cyber-attacks-and-terrorism-top-security-strategy-priority.htm.

[96] *See* Peter P. Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, 153 U. Pa. L. Rev. 1975, 1977 n.4 (2005) (noting the strikingly low level of cybersecurity discussion, other than encryption, in Internet policy discussions throughout the late 1990s).

significant attention in preparation for the Y2K problem[97] and in response to distributed denial of service attacks on popular e-commerce websites during early 2000.[98] 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 measures being implemented later, if at all. One sign of a change emerged in 2002 when Microsoft stopped all development on its Windows operating system in order to provide engineers with eight weeks of intensive security training.[99] 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 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.[100]

This increased attention to cybersecurity is relevant to encryption debates today. In the late 1990s there was little awareness of the importance and challenges of cybersecurity. Today, those concerns are widely acknowledged and addressed. This Part of the Article explains why encryption is vital to cybersecurity and relevant to the many challenges facing nations globally today.

[97] Y2K is shorthand for the Year 2000 Problem, which referred to the potential malfunction of computer operating systems on January 1, 2000. The fear was that information technology systems would misread the change in century as 1900 instead of 2000, causing errors that would disrupt and potentially shut down information systems across the world. Fortunately, these fears were largely unfounded. "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*, Wash. Post, May 16, 2003, http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html.

[98] The denial of service attacks in 2000 prompted the Department of Justice to host a cybercrime "summit." Attorney General Janet Reno, Address at the Stanford University Law School Cybercrime Summit: A Law Enforcement/Information Technology Industry Dialogue on Prevention, Detection, Investigation and Cooperation, Speech at the Cybercrime Summit (Apr. 5, 2000) (*transcript available at* http://www.justice.gov/archive/ag/speeches/2000/4500agcybercrimes.htm).

[99] Microsoft imposed a two-month security stand down from February to April 2002. *See The Journey to Trustworthy Computing: Microsoft Execs Report First-Year Progress*, Microsoft (Jan. 15, 2003), http://www.microsoft.com/presspass/features/2003/jan03/01-15twcanniversary.mspx.

[100] Memorandum from Bill Gates to Microsoft and Subsidiary Employees, Trustworthy Computing, Microsoft (Jan. 15, 2002, 02:22 PM), http://www.microsoft.com/about/companyinformation/timeline/timeline/docs/bp_Trustworthy.rtf.

2. Cybersecurity and the increasing importance of computing of the Internet

The rise of cybersecurity as a policy issue is a direct result of global reliance on computing and the Internet. This conclusion is likely intuitive to most readers. The recent and steep increase in e-commerce illustrates this growth. In 1998, the best available estimates of e-commerce revenue were less than $1 billion per year.[101] In 2010, however, online retail sales exceeded $172 billion in the US alone and were estimated to continue growing to $250 billion in the US by 2014.[102] The range of activities conducted online has similarly multiplied for personal, business, and governmental organizations.

Globalization also expands the range of nations in which the Internet and computing play an essential role in society. In 1998, both India and China had fewer than 2 million Internet users each.[103] Today, however, even a conservative estimate shows that over 100 million people are connected to the Internet in India[104] and over 485 million in China.[105] Accompanying this globalization of the Internet are intensive cross border transfers of information. For example, India's IT business process outsourcing (BPO) sector has grown rapidly: as a proportion of India's national GDP, sector revenues have increased from 1.2 percent in 1998 to an estimated 6.4% in 2011, accounting for an estimated $88.1 billion USD in aggregate revenue.[106] This back-office sector now accounts for over

[101] Peter P. Swire & Robert E. Litan, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive 64 n.13 (1998) (citing *Questions Surround SET Pilots*, Electronic Commerce News (Aug. 18, 1997)).

[102] Erick Schonfield, *Forrester Forecast: Online Retail Sales Will Grow To $250 Billion By 2014,* Techcrunch.com, (Mar. 8, 2010), http://techcrunch.com/2010/03/08/forrester-forecast-online-retail-sales-will-grow-to-250-billion-by-2014/.

[103] *See Internet Usage Stats and Telecommunications Market Report*, Internetworldstats.com, http://www.internetworldstats.com/asia/in.htm (last updated Apr. 9, 2011); *Evolution of Internet in China,* China Education and Research Network (Jan. 1, 2001), http://www.edu.cn/introduction_1378/20060323/t20060323_4285.shtml.

[104] *See E-Commerce is Booming in India: Rajan Anandan, Head, Google's India Operations*, Econ. Times (Aug. 9, 2011), http://articles.economictimes.indiatimes.com/2011-08-09/news/29867320_1_rajan-anandan-e-commerce-internet-users.

[105] *See China Web Users Hit 485 Million*, Reuters.com (July 9, 2011), http://www.reuters.com/article/2011/07/19/us-china-internet-idUSTRE76I12020110719.

[106] *See* NASSCOM, The IT-BPO Sector in India Executive Summary 5 (2011), http://www.nasscom.in/sites/default/files/researchreports/Exec%20Summary_0.pdf

25% of India's total exports.[107] The twin phenomena of greater Internet use and increased transborder activity means that actions taken by non-U.S. countries have more vital effects on U.S. businesses and organizations.

3. The pervasive use of cryptography today

As society becomes increasingly interconnected, cryptography facilitates the preservation of security and privacy in everyday life. Encryption is not merely used to protect communications or stored data. This is a commonly held misperception, which understates the prevalence of encryption in everyday life. In fact, encryption is the norm, not the exception, and is used in innumerable ways—from protecting critical public infrastructure and sensitive personal information, to securing communications and commercial transactions. Cryptographer Matt Blaze sums up the current state of encryption today in this way: "The transparent use of cryptography by everyday people (and criminals) has, in fact, exploded. Crypto software and algorithms . . . can now be openly discussed, improved and incorporated into products and services without the end user even knowing that it's there."[108]

To illustrate this point, consider a typical day in life of Alice. As Alice backs out of her driveway, she quickly closes the garage door with a remote control. On her way to work, Alice stops by her local Starbucks and purchases a coffee with her credit card. She then drives to the local train station and swipes her smart card to board a train into the city. While on the train, Alice calls her client Bob using her new smart phone. With her hands full, Alice decides to switch to her wireless Bluetooth piece. After arriving at her train stop, Alice walks a couple blocks to her work building, swiping her entry card to unlock the door. Finally at her desk, Alice logs into the company network by typing in a password. At each step of Alice's morning, she has used encryption-enabled devices—all before 9:00 am.

As described in the example above, encryption is used in the background of most transactions, with the user blithely unaware of its presence. One widely deployed encryption system is SSL, or Secure Sockets Layer. SSL is a protocol that establishes a secure session link between a website and a user's web browser. All communications and data sent through this link are secured with a cryptographic hash, using digital certificates. SSL is widely used for online shopping and banking, and also to protect many emails

[107] *Id.*

[108] Matt Blaze, *Wiretapping and Cryptography Today*, Matt Blaze's Exhaustive Search (July 12, 2011), http://www.crypto.com/blog/wiretap2010.

globally that use webmail systems. HTTPS is an SSL application that is integrated into most web browsers and provides protection for information transmitted to SSL-enabled web servers.[109] Another common use of encryption is a Virtual Private Network (VPN), which uses authentication and encryption to secure connections between a remote user and an organization's network.[110]

Software-based encryption is also used to protect data at rest, such as information stored on a personal computer. This capability is standard in most computers sold today, such as through Microsoft's Bit Locker and Apple's FileVault.[111] Encryption is also often provided at the hardware level, such as through the Trusted Platform Module (TPM), discussed above in connection with its exclusion from China[112]

The proliferation of encryption today illustrates its importance to the basic functioning of modern computing. Limiting the use of effective encryption would disrupt our everyday lives and undermine security for our pervasively online world.

4. The offense is ahead of the defense, making encryption vital to cybersecurity

A fundamental problem with cybersecurity today is that the offense is ahead of the defense.[113] "Offense" refers to the hackers who wish to penetrate and disrupt or exploit a cyber system. "Defense" refers the owners and users who wish to protect their cyber systems from intrusion. Cyber attacks have grown rapidly in recent years, increasing in both number and sophistication. These threats are exacerbated by the interconnectedness of the comput-

[109] For a description of SSL technology and its specifications, see Alan O. Freier & Phillip Karlton, *The SSL Protocol Version 3.0* (Nov. 18, 1996), *available at* http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00.

[110] *See* Michael Stines, *Remote Access VPN – Security Concerns and Policy Enforcement*, Sans Institute (2003), http://www.sans.org/reading_room/whitepapers/vpns/remote-access-vpn-security-concerns-policy-enforcement_881.

[111] *See About FileVault*, http://docs.info.apple.com/article.html?path=Mac/10.6/en/8727.html (last visited Mar. 13, 2012) (providing a basic overview of Apple's FileVault encryption system); *BitLocker Drive Encryption Overview*, http://windows.microsoft.com/en-US/windows-vista/Bit-Locker-Drive-Encryption-Overview (last visited Aug. 1, 2011).

[112] *See generally* TCG Best Practices Committee, *Design, Implementation, and Usage Principles Version 3.0*, Trusted Computing Group (Feb. 2011), *available at* http://www.trustedcomputinggroup.org/files/resource_files/5B50FA87-1A4B-B294-D0054DD2BACDF801/Best_Practices_Principles_Document_v3%200_Final.pdf (providing a detailed explanation of TPM technology).

[113] *See generally* Dep't of Def., *Department of Defense Strategy for Operating in Cyberspace* (July, 2011) 1-4, *available at* http://www.defense.gov/news/d20110714-cyber.pdf (describing the many cybersecurity threats that exist today).

ing environment today. In this era of generally weak defense, encryption is the preeminent defensive tool.

Cyber attacks differ in important respects from attacks in the physical world.[114] 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 one's "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.[115]

Second, cyber attacks are cheap while defense is costly. Hacking technology is widely available and, because attacks can be launched remotely, the offense incurs only nominal expense. Meanwhile, the defense is only as strong as its weakest point.[116] Because attacks can be launched from anywhere on the web, defenders have to expend valuable resources in hopes of maintaining good security at every point. The defense needs to be strong everywhere, while the offense only needs to succeed in one place.

Third, cyber attacks can be launched repeatedly. A physical burglar has to wait for the right moment to try to enter a house. But a remote hacker can search for vulnerabilities 24 hours a day, and can use automated attacks to continuously probe for weaknesses.

Fourth, the source of attack is often difficult to determine. The apparent source of attack is often not the actual source.[117] The ability to disguise the source of an attack greatly inhibits deterrence, because the defense often has no feasible way to locate and punish the attacker.[118]

[114] *See generally* Peter P. Swire, *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?* 3 J. Telecomm. & High Tech. L. 163 (2004) (discussing the differences of cyber attacks versus attacks in the physical world.).

[115] *See generally* Nimrod Kozlovski, *A Paradigm Shift in Online Policing - Designing Accountable Policing* (June 2005) (unpublished J.S.D. dissertation, Yale Law School), *available at* http://crypto.stanford.edu/portia/papers/Kozlovski.pdf (discussing the general nature of cyber crime).

[116] "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 25, at 5 (emphasis in the original).

[117] 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.

[118] Deterrence was an essential feature of the Cold War between the Soviet Union and the United States. Under the theory of mutually assured destruction, a potential attacker knew that its missiles could be traced back to the

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, the offense 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. Cryptography 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. Similarly, for data at rest, encryption protects files residing inside an individual's or organization's computer system. Penetration of the system by an attacker typically does not compromise the encrypted files.[119] In addition, cryptography is built into the essential function of authentication over the Internet.[120]

The usefulness of strong encryption underscores the main problems with prohibiting encryption or deploying weak encryption. For data in motion, Figure 3 illustrates an essential fact about the Internet—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.[121] In authentication, lack of encryption allows a hacker to read the password or other identification information used in the

source and that the enemy could then identify and retaliate against the initial attacker. *Nuclear Age-Mutual Assured Destruction*, Science Encyclopedia, http://science.jrank.org/pages/10504/Nuclear-Age-Mutual-Assured-Destruction.html (last visited Aug. 7, 2011). In cyber attacks, however, the initial source of the attack can often mask itself by routing the attack through multiple intermediate Internet locations. These locations may not be aware or approve of the attack, and are an inappropriate target for retaliation. *See* Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, Sci. Am. (June 11, 2011), http://www.scientificamerican.com/article.cfm?id=tracking-cyber-hackers.

[119] The ability of an attacker to penetrate a system could potentially result in compromised data if the attacker is able to learn the encryption keys or otherwise obtain authority to access the encrypted files.

[120] *See RSA Authentication Manager Express*, *supra* note 18 (providing information about RSA's widely used two-factor authentication system).

[121] For example, Massachusetts sets forth strict penalties for loss of a laptop or other data unless strong encryption is in place. Mass. Gen. Laws ch. 93H (2007); Mass. Gen. Laws ch. 93A. *§ 4* (2007). Most states do not require notice in the event of a data breach of effectively encrypted data.

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.[122]

Cyber security defenders do have other techniques to protect themselves from attacks. One way to stop remote attacks is to disconnect from the Internet altogether. Some military and other sensitive networks secure themselves by using an "air gap" to create separation from the Internet.[123] Though this separation provides security, it also comes at the high cost of convenience and functionality. Firewalls are another important category of defensive tools used to protect networks from unauthorized access, while still permitting legitimate communications to enter. Such firewalls are essential to protecting an organization's systems from certain outside attacks. They 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 cryptography.

In conclusion, effective encryption is now a pervasive and preeminent element of cybersecurity. For data in transit, data at rest, and authentication, there is no effective substitute. Any legal regime that prohibits the use of strong encryption thus significantly undermines and harms 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, regardless of their geographic location.

Key escrow provides a vivid example of the least trusted country problem. Based on interviews in 2011 with Government of India officials, India has seriously discussed requiring key escrow.[124] The many failings of key escrow were discussed earlier in this Arti-

[122] *See* discussion of SSL, *supra* Part IV.A.3.

[123] An "air gap" is a network security mechanism in which high security networks are completely isolated from connection to a less secure system.

[124] Swire Interviews, *supra* note 66.

cle. Suppose that India adopts this approach, and that other countries follow suit. The least trusted country problem is essentially a thought experiment—how secure would India feel if Pakistan could also access the escrowed keys? In this situation, Indian's sensitive communications would be exposed to a country with which it has a violent history and strained relationship. The same logic applies to whatever country a person trusts least, such as China and Taiwan, Israel and Iran, and so on.

The least trusted country problem extends to other limits on encryption. Current law in India limits encryption to a 40-bit key —a key-length so weak and outdated that it was trivially easy to break over a decade ago.[125] As discussed above, this limit on encryption was rarely enforced before the 2008 attacks on Mumbai. More recently, in the wake of the disputes with RIM and other companies, it is unclear how strictly the government will enforce limits on encryption. Regular enforcement of these rules, however, would weaken the Internet globally. India's BPO sector helps illustrate this problem. Back-office service companies routinely transmit health, financial and other sensitive information to and from the United States, Europe, and other countries. In the absence of strong encryption to protect this data, the prudent assumption is that this data will be easily compromised. As a global leader in the business processing industry that regularly transmits sensitive data, and with a population of over one billion people, a massive volume of Internet and other communications would be subject to compromise.

A similar analysis applies to use of unproven and homegrown encryption algorithms in China, which has its own large population and significant Internet use. Experienced cryptographers know not to trust a cryptosystem until it has undergone rigorous and repeated testing through a public peer review process. Unproven algorithms also have a much higher risk of containing secret backdoors. Internet communications that originate or end in China using those algorithms should be presumed compromised. If unproven algorithms are used in hardware, such as for computer chips, then devices using those chips should also be presumed compromised. Magnifying the risk to cybersecurity, vendors who wish to do business in China may be required to incorporate the unproven algorithms into products and services used outside of the country. In this situation, one nation's use of weak encryption would undermine the overall security of the Internet more generally.

Ultimately, laws that limit effective encryption create security holes. Communications that originate, end, travel through, or com-

[125] Blaze, *supra* note 21 (describing low cost and short time needed to break a 40-bit key).

ply with the policies of those nations are systematically weakened —they are as secure as they would be in the hands of our least trusted country, whatever country that may be.

This analysis illustrates how globalization increases the importance of strong encryption. During the 1990s, the U.S. government discussed helping other countries establish key escrow regimes. The focus of discussion, however, rested on how key escrow could operate within the United States. [126] Policymakers debated the level of trust that could be placed in independent key recovery organizations within the U.S., considering its history of civil liberties and the rule of law. Even in that setting, the arguments against key escrow were far more persuasive than those in favor of such a regime.

The arguments against key escrow, or other limits on effective encryption, are even more persuasive in a world where several, or 20, or 200 countries impose such limits. If keys are held in numerous countries, then there are many potential points of compromise. A key recovery organization may relinquish the keys even in the absence of court orders or other rule-of-law protections. An "independent" organization might be coerced to turn over the keys to the local government. Criminals or others might corrupt insiders at the organization, effectively placing 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 would result from limits on strong encryption.

V. 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 strong encryption is used without restrictions, and (3) the use of encryption regulation as a tool for advancing international trade. In response, this Part will assert that: (1) there are compelling 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.

[126] Abelson et al., *supra* note 40, at 7, 11, 14 (discussing the international ramifications of key escrow).

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

As discussed above, a "backdoor" provides the creator of software or hardware with access to data without the permission or knowledge of the user. During 2011 interviews conducted with Indian government officials, a commonly voiced concern was that surveillance agencies in the U.S. and other countries are granted access into allegedly strong commercial encryption systems via backdoors but that other nations are denied similar access.[127] If true, this would serve as an understandable rationale for India and other countries lacking backdoors to impose limits on the use of strong encryption. Otherwise, this system of selective access would be unfair and could pose a national security risk to those countries lacking such access.

1. It is difficult to keep backdoors secret

Backdoors are inherently insecure. The purpose of a backdoor is to enable access for legitimate actors (the "good guys"), but deny access to all others (the "bad guys"). With encrypted systems, however, there is a wide range of actors who may discover a backdoor. Attackers, for instance, may include Ph.D. computer security experts who benefit professionally from exposing security weaknesses. 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.[128] Other potential attackers include criminals, including large organized crime operations that possess ample resources to attract costly computer security talent, or foreign governments.[129] In addition, the creators of backdoors have to worry about insider attacks—the possibility that an insider who helped create the backdoor will disclose the secret. To illustrate this point, consider the Wikileaks disclosures in 2011. The leak of hundreds of thousands of U.S. government classified messages, allegedly from an insider, exemplifies the difficulty of keeping secrets in the Inter-

[127] Swire Interviews, *supra* note 66.

[128] *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. *See* Carnegie Mellon University's Computer Emergency Response Team, www.cert.org (last visited Aug. 10, 2011).

[129] *See, e.g.*, Press Release, Dep't of Just., *Organized Romanian Criminal Groups Targeted by DOJ and Romanian Law Enforcement* (July 15, 2001), *available at* http://www.justice.gov/opa/pr/2011/July/11-crm-926.html (detailing an organized cyber crime investigation in Romania).

net age.[130] In assessing the likelihood of backdoors in the globally standard encryption systems, it is highly significant that no backdoors have been discovered in globally used encryption standards since the 1999 shift in U.S. encryption policy.[131] In our modern Wikileaks world, with so many potential attackers, this lack of discovered backdoors is important evidence that they do not exist.

Similarly, businesses have strong incentives not to implement backdoors in their encryption products. Consider this example—assume a multinational technology corporation such as Microsoft or Apple developed an encryption product with a secret backdoor, allowing access to user data or communications.[132] If such a backdoor were discovered, the company would incur severe civil and criminal penalties across the world, in addition to irreparable damage to its brand name, loss of consumer trust, and drop in market value. The companies' incentives thus provide important security for users of the commercial cryptosystem.

This analysis illustrates the difficulty of maintaining a secret backdoor in encryption systems and other widely used software that is subject to public scrutiny. Because modern cryptosystems are subject to repeated attacks by a wide range of sophisticated attackers, the likelihood of a backdoor remaining secret over time is low.[133]

2. Law enforcement can sometimes circumvent encryption without backdoors

Law enforcement and intelligence agencies can still outmaneuver criminals and other malicious actors by use of intercept methods that do not compromise cryptosystems. One such method is to intercept data before it is encrypted. For example, an agency might access Alice's system with a hidden camera or a keystroke logger

[130] "WikiLeaks is a whistle-blowing website that became the focus of a global debate over its role in the release of thousands of confidential messages about the wars in Iraq and Afghanistan and the conduct of American diplomacy around the world." *Wikileaks,* N.Y. Times, http://topics.nytimes.com/top/reference/timestopics/organizations/w/wikileaks/index.html, (last updated Feb. 27, 2012).

[131] Basic encryption algorithms such as RSA and AES have been subject to public peer review for well over a decade. If white hat attackers had discovered backdoors in those algorithms, it is safe to assume that this information would have been made public, if only when a patch for the backdoor was deployed.

[132] Microsoft deploys the encryption software BitLocker in its Windows software. The comparable Apple product is FileVault. *See About FileVault, supra* note 111; *Bitlocker Drive Encryption Overview, supra* note 111.

[133] Peter P. Swire, *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?* 3 J. Telecomm. & High Tech. L. 163 (2004).

that logs everything typed on her computer keyboard.[134] 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.[135] 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. These three potential points of compromise—at the sender, recipient, or at the telephone network—provide law enforcement and national security agencies with advantages in lawful interception, without relying on any weakness or flaw in the cryptosystem itself.

Another category of compromise exists at the implementation stage of an encryption system. Even with an unbreakable cryptosystem, subtle security issues arise at the practical implementation level, such as when particular devices or software must operate together. 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-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."[136] As an open source library, OpenSSL is used globally, including with the substantial fraction of web servers that use Apache software.[137] 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.[138] Because implementation remains difficult even with strong encryption, intelligence agencies may discover weaknesses in existing, implemented systems.

[134] A keystroke logger is a type of spyware that tracks, or logs, the keystrokes of a user, typically covertly.

[135] A rootkit is software that accesses computer functions, hidden from the operating system and security software.

[136] Apache HTTP Server Project, http://httpd.apache.org/ (last visited Aug. 3, 2011).

[137] As of August 2011, the Apache HTTP open-source web server had over 65 percent of the web server market share. *August 2011 Web Server Survey*, Netcraft.com, (Aug. 5, 2011), http://news.netcraft.com/archives/2011/08/05/august-2011-web-server-survey-3.html#more-4797.

[138] *Security Updates*, Apache HTTP Server Project, http://httpd.apache.org/security_report.html (last visited Aug. 1, 2011) (Information on security problems fixed in released versions of the Apache HTTP Server).

3. There is a greater likelihood of backdoors existing in encryption systems that have not been publically tested

This discussion has thus far only addressed encryption systems subjected to sustained testing over a long period of time. This sort of public 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, dating back to the 1883 writings of Auguste Kerckhoff, who stated, "[t]he system must not require secrecy and can be stolen by the enemy without causing trouble."[139] 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 time.

This empirical approach to assessing the strength of an encryption system is directly related to the probability of a secret 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 homegrown cryptosystems based on algorithms that have not been subjected to significant peer review.[140] Without such testing, users of these encryption systems cannot rule out the existence of intentional backdoors. This risk makes it perilous for such commercial systems to be deployed globally. 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.

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

A persistent concern for law enforcement and national security is that the agencies are "going dark"—new forms of communications are traveling through channels 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

[139] Steve Bellovin, *Security through Obscurity*, Risks Digest (June 6, 2009, 10:21 PM), http://catless.ncl.ac.uk/Risks/25.71.html#subj19 (referring to Kerckhoffs' second principle).

[140] *See supra* Part III.B.2.c (for more information on Chinese homegrown encryption standards).

that they previously relied upon. The discussion here, however, argues that this 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, law enforcement and intelligence agencies' surveillance capabilities are actually greatly enhanced by the current mix of new technologies. Thus the "going dark" concern is not a convincing reason 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 surveillance capabilities that they previously relied upon. The use of wiretaps and relatively easy access to stored records have historically served as important investigatory 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:

> 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.[141]

[141] House Judiciary Comm., Subcomm. on Crime, Terrorism, and Homeland Security, Statement by Valerie Caproni, FBI General Counsel, Going Dark: Lawful Electronic Surveillance in the Face of New Technologies (Feb. 17, 2011), *available at* http://judiciary.house.gov/hearings/pdf/Caproni02172011.pdf. Caproni used the term specifically in reference to CALEA-style problems. *Id.* at 1. Caproni's quote in the text, however, shows that the real objection is broader, applying to "the gap between authority and capability." *Id.* This Article thus uses the term "going dark" to refer to the full range of gaps between authority and capability, notably: (1) CALEA-type problems where lawful process does not provide access to a communications; (2) issues when strong encryption is used for communications, where law enforcement retrieves the communication but can-

"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 wish *justice* to be "blind," in order to achieve impartiality, we surely do not want our police to be blind.

In the 1990s, the FBI and NSA often used the "going dark" argument as justification for imposing limits on encryption, although the term itself was not widely used.[142] In 1994, CALEA was enacted to address FBI concerns that the shift from copper wires to fiber optics was making traditional wiretaps less useful. During this period, the NSA's ability to collect communications was threatened as a greater proportion of international calls shifted from radio communications (generally easy to intercept) to fiber-optic cables (generally hard to intercept except at a phone company switch). With the rapid development and widespread availability of strong encryption, the agencies feared that communications would become increasingly inaccessible. The Clipper chip was one proposed remedy to these challenges.

Despite these risks, the U.S. government eventually embraced the use of strong encryption in 1999. 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 it identified the inherent value in using strong encryption for law enforcement and national security purposes. Despite "losing" the crypto wars, agency concerns were still addressed. The FBI received additional funding for its technical interception capabilities, which has continued to grow over time.[143] Together, government and industry leaders worked to develop the system of public-private partnership that continues today, in which industry experts coordinate with the government to address encryption, technology, and legal intercept issues.[144]

not decrypt it; and (3) issues with strong encryption at rest, where law enforcement gains access to a laptop or other device but cannot decrypt the stored information.

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

[143] The proposal authorized additional funding of $80 million over four years to the FBI for its Technical Support Center, a resource intended to aid all levels of law enforcement with their technical surveillance initiatives. The White House, *The Cyberspace Electronic Security Act of 1999*, § 207 (Sept. 16, 1999), *available at* http://www.epic.org/crypto/legislation/cesa/bill_text.html. After the September 11, 2001 terrorist attacks, the USA PATRIOT Act of 2001 authorized an increase in funding to $200 million over three years.

[144] For example, the U.S. government conducts outreach through public-private partnerships such as the Communications Security, Reliability and

The "going dark" concern has recently resurfaced in the United States, in connection with FBI support for revising the 1994 CALEA statute. Agencies today must contend with new and rapidly evolving communications technologies, ranging from online social networks and new mobile platforms to video games.[145] In place of the old monopoly telephone network, agencies also have to deal with a confusing variety of communications providers, some of which have little experience with legal process compliance. Agencies, in the U.S. and globally, are thus concerned that they will fall behind and "go dark."

2. Today is a "golden age for surveillance"

Technological innovation repeatedly presents obstacles to lawful interception. At the same time, these technological developments provide law enforcement and national security agencies with powerful new surveillance capabilities. The discussion here highlights three areas where law enforcement has far greater surveillance capabilities than ever before in history: (1) location information; (2) information about contacts and confederates; and (3) an array of new databases that establish "digital dossiers" about an individual's life.[146] This information is made even more useful because of the way that data mining can help identify suspects.

We are entering a new age in which most individuals carry a tracking device, the mobile phone. Location tracking is a standard feature in a wireless network—the phone company needs to know where your phone is located to route calls to you. Location information is tremendously useful for law enforcement and national

Interoperability Council (CSRIC), the Network Reliability and Interoperability Council (NRIC), and the National Infrastructure Protection Plan. *See* Communications Security, Reliability and Interoperability Council, http://www.fcc.gov/pshs/advisory/csric/ (last visited Aug. 5, 2011); Network Reliability and Interoperability Council, http://www.nric.org/ (last visited Aug. 5, 2011); and National Infrastructure Protection Plan, www.dhs.gov/nipp (last visited Aug. 5, 2011).

[145] Online video games, such as World of Warcraft, now incorporate chat and voice capabilities. *See, e.g., Voice Chat FAQ*, Battle.net, http://us.battle.net/support/en/article/voice-chat-faq#q-1 (last visited Apr. 13, 2012). Although parents may complain that video games are a colossal waste of their children's time, investigatory agencies view the video game in even more stark terms—a new international channel to facilitate terrorist and criminal communications. Yet video game technology is not subject to government scrutiny before the games can be marketed. The sheer volume and variety of communication technology thus continues to grow. At any given moment, many of those new technologies will not have an established method of access for law enforcement, even with a court order or other lawful process.

[146] *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083 (2002).

security agencies. It can put a suspect at the scene of a crime, or establish an alibi. Mobile phones can also act as a "bug" for law enforcement, eliminating the need or risk for a physical bug to be placed on the suspect's person or property.

The precise rules for storing location data vary by jurisdiction and wireless carrier. In many instances, however, location data is routinely stored for a significant period of time.[147] Carriers in the U.S. are subject to data preservation orders, so that relevant location information is retained once a proper agency request has been made.[148] The number of requests from law enforcement for such location information in the U.S. has climbed sharply in recent years.[149]

It is true that a cautious suspect may avoid location tracking, such as by using an unidentifiable prepaid cell phone or by abstaining from using a phone during criminal activities. However, some countries impose limits on non-identifiable mobile phones.[150] Also,

[147] Law enforcement and data protection agencies within the European Union continue to debate data retention policy. *See, e.g.,* Letter, European Digital Rights, et. al, Joint Letter on Data Retention (August 26, 2011), *available at* http://www.edri.org/files/dr_letter_260911.pdf (arguing that proposed data retention legislation would violate fundamental human rights); Response to European Digital Rights' Joint Letter on Data Retention, Cecilia Malmstrom, Member of the European Commission (October 31, 2011), *available at* http://www.edri.org/files/malmstroem_letter31Oct2011.pdf; Press Release, European Data Protection Supervisor, Evaluation shows that the Data Detention Directive does not meet privacy and data protection requirements, says EDPS (May 31, 2011), *available at* http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-06_Data%20Retention %20Report_EN.pdf (detailing the European privacy agency's opinion that the Data Retention Directive of 2006 fails to meet the requirements of fundamental rights to privacy and data protection). The Data Retention Directive of 2006 requires retention of phone records for six to 24 months. Council Directive 2006/24/EC, art. 6, 2006 O.J. (L 105) 54, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do? uri=CELEX:32006L0024:EN:HTML. In the United States, data retention bills have advanced in the Congress, but have not become law as of 2012. *See, e.g.* H.R. 1981, 112th Cong. (2011).

[148] Data preservation laws in the United States require providers of electronic communication services or remote computing services to preserve data upon government request, for 90-day renewable periods. 18 U.S.C. § 2703(f) (2012).

[149] *See* Press release, ACLU, ACLU Seeks Details on Government Phone Tracking in Massive Nationwide Information Request (Aug. 12, 2011), *available at* http://www.aclu.org/technology-and-liberty/aclu-seeks-details-government-phone-tracking-massive-nationwide-information-0.

[150] Purchase of a mobile phone in India, for instance, requires photo identification and registration of the phone with the government. *See Subscriber Verification*, Cellular Operators Ass'n of India, http://www.coai.in/projectDetails.php?id=3 (last visited Aug. 23, 2011).

a suspect can only control his or her own actions—there are obvious limits to controlling whether criminal confederates use the same anti-tracking precautions. More generally, a majority of people now carry and use cell phones in their daily lives. Location information is thus available for surveillance purposes in historically unprecedented ways.

Information about one's contacts is the second category of information newly available to agencies. In many investigations, the identities of the implicated parties are just as important as the content of the communication. Equipped with identity information, the investigator can easily retrieve leads on whom else to investigate, and can follow those leads to a suspect's contacts, and so on.

The importance of confederates and contacts has become especially famous through online social networking. The term "social graph" was coined, in connection with Facebook and other social networks, to describe "the global mapping of everybody and how they're related."[151] For investigatory agencies, the mapping of social relationships is extremely useful. Social networking sites themselves will become an increasingly important source of investigatory material in coming years. The current trend, however, is much more general:

- *Long-distance and international phone calls.* A generation ago, long-distance phone calls were expensive, and international calls were a rare and costly affair. As costs plummeted, the volume of local, long-distance, and international calls grew significantly over time.[152]
- *To/from information.* Calling records show the to/from information for calls made—pen-register orders reveal the identity of the person one is calling, and trap-and-trace orders disclose the identity of the caller. The number of these legal orders in the U.S. has climbed sharply over time.[153]

[151] Brad Fitzpatrick, *Thoughts on the Social Graph*, Bradfitz.com (Aug. 17, 2008), http://bradfitz.com/social-graph-problem/.

[152] The per-minute charge in the United States for calls made outside the United States fell 83% from 2000 to 2009, from $0.47 per-minute to $0.08 per-minute. *See* Press Release, FCC releases 2009 International Traffic Data (Apr. 8, 2011), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-305658A1.pdf.

[153] For foreign intelligence investigations, the government made 24,287 National Security Letter (NSL) requests in 2011, compared with a very small number a decade earlier. Letter from Assistant Atty. Gen. Ronald Weich to Majority Leader Harry Reid (Apr. 29, 2011), *available at* http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf; U.S. Senate Jud. Comm. Subcomm. on the Const., Statement by Peter P. Swire, Responding to the

- *Mobile phones.* Mobile use continues to increase—India, for instance, had over 20 million new wireless subscribers in March 2011.[154]
- *E-mails.* The number of worldwide email accounts increased from 891 million in 2000 to over 2.9 billion in 2010.[155] By 2014, this number is projected to increase to over 3.8 billion.[156] The emergence of free or low-cost global webmail providers, such as Gmail, Yahoo, and Hotmail, provides investigatory agencies the convenience of serving many lawful requests to a small number of providers.
- *Text messages.* The rise of unlimited text messaging plans in many jurisdictions provides numerous clues about a person's key contacts and the time and date of their communications.
- *VOIP (Voice over Internet Protocol).* In 2011, Microsoft acquired Skype for $8.5 billion.[157] Although Skype calls are encrypted end-to-end, its to/from information is still subject to legal process.

These wireline and wireless calls, e-mails, texts, VOIP communications, and social networking records are treasure troves of information for investigatory agencies seeking information about a suspect's confederates. In the bygone era of face-to-face communications, meetings left no trace of the suspect's contacts. Today, by contrast, an individual would need to abstain from many everyday activities to prevent the government from obtaining information about his or her contacts. The identity of those contacts helps lead investigators to additional targets of interest, thereby painting a

Inspector General's Findings of Improper use of National Security Letters by the FBI (Apr. 11, 2001), *available at* http://www.judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862f735da124b3b9&wit_id=e655f9e2809e5476862f735-da124b3b9-0-4.

[154] Press Release, Telecom Regulatory Authority of India, Highlights of Telecom Subscription Data as on 31st March 2011 (Apr. 29, 2011) *available at* http://www.trai.gov.in/WriteReadData/PressRealease/Document/Press_Release_Mar-11.pdf

[155] *See* John Fontana, *Email continues explosive growth*, Network World Fusion, March 8, 2001 http://www.networkworld.com/news/2001/0308email.html; See also The Radicati Group Inc., Email Statistics Report 2010–2014 Executive Summary 2 (April 2010) http://www.radicati.com/wp/wp-content/uploads/2010/04/Email-Statistics-Report-2010-2014-Executive-Summary2.pdf.

[156] *Id.*

[157] Press Release, Microsoft, Microsoft to Acquire Skype (May 10, 2011), *available at* http://www.microsoft.com/presspass/press/2011/may11/05-10corpnewspr.mspx.

broader and more precise picture of potential criminal or national security activity.

Location and contact information, in turn, are simply examples of the larger trend towards the retention of detailed personal records. Consider the amount of information stored on an individual's personal or work computer. Today, a standard laptop often retains many gigabytes of data, more than a mainframe computer could hold 20 years ago.[158] 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 personal records. The records retained on that computer 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 new tools for identifying suspects and their contacts. Law enforcement and national security agencies now have sophisticated data mining capabilities in-house, or can contract with the private sector for such capabilities.[159]

3. Choosing between "going dark" and a "golden age for surveillance"

This Article argues that the big picture for agency access to data today is "golden" rather than "dark." The loss of access caused by encryption is more than offset by the surveillance gains from new computing and communications technology. In addition, government regulation of encryption harms cybersecurity and results in the least trusted country problem discussed above. Investigatory agencies will not easily accept these conclusions, however, so it is important to work through the analysis in more detail.

[158] Peter P. Swire, *The Consumer as Producer: The Personal Mainframe and the Future of Computing*, 42 World Jurist Ass'n Law/Tech., 1st Quarter (2009) at 8, n. 3.

[159] *See* Robert O'Harrow Jr., No Place to Hide (2005) (providing a comprehensive investigation of private sector data mining offerings to the U.S. government). *See also* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 Harv. C.R.-C.L. L. Rev. 435 (2008).

Agencies do face the technological innovation that creates gaps in lawful process. However, implementing wiretaps and accessing plaintext data are not the only relevant policy goals. The computing and communications infrastructures are vital to economic growth, private sector innovation and government operations, and are relied upon by the investigatory agencies themselves. If there is modest harm and enormous gain to be derived from using certain technology, societies should logically adopt that technology. In 1999, the U.S. government concluded that strong encryption was precisely that type of valuable technology—it was worth going at least slightly "dark" in order to reap the many benefits of effective encryption. Strikingly, government support of strong encryption did not waver even after the terrorist attacks of September 11, 2001.

Evidence further suggests that, despite the widespread use of strong encryption, wiretaps have become more useful over time. The number of wiretap orders implemented in the United States has in fact grown steadily over the last two decades. According to publicly available statistics, court approved wiretaps are now at a record high.[160] Three thousand, one hundred and ninety-four wiretap court orders were issued for the interception of electronic, wire, or oral communications in 2010. In the six instances where encryption was encountered in 2010, the encryption did not prevent law enforcement from retrieving the plaintext forms of communication.[161]

These numbers actually understate the expansion of wiretapping in the U.S., in part due to the adoption of "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.[162] Roving wiretaps thus decreased the number of separate court orders reported in official

[160] Admin. Office of the U.S., *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications,* June 2010, at 6, *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2010/2010WireTapReport.pdf. [hereinafter Wiretap Report 2010] 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) (2012).

[161] Wiretap Report 2010, *supra* note 160, at 9. Public Law 106-197 amends 18 U.S.C. § 2519(2)(b) to require the inclusion of wiretaps for which encryption was encountered and whether encryption prevented law enforcement from obtaining the plaintext of the intercepted communication. Pub. L. No. 106-197, 114 Stat. 247 (2000).

[162] *See* 50 U.S.C. § 1805(c)(2)(B) (2012). *See also* 18 U.S.C. § 2518(11)–(12) (2012).

statistics.[163] Also, wiretaps are now authorized by investigation, rather than for each individual target within an investigation. This similarly implies that official statistics understate the actual growth in wiretap use.

How can the investigatory agencies' sense of loss be explained when, in fact, (1) wiretap use is expanding; (2) encryption has not been an obstacle to wiretaps; and (3) agencies now have powerful, new surveillance tools at their disposal? One explanation derives 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.[164] This concept of loss aversion also helps to explain the "endowment effect"—the theory that people place a higher value on goods they own versus comparable goods they do not own.[165] When applied to surveillance capabilities, these theories help explain why agencies feel losses much more acutely than newly acquired gains. Whether based on the academic theory or simply on common sense, we often take for granted the good things that come our way and instead focus on the negative, even when the good significantly outweighs the negative.

Similarly, one consequence of loss aversion is "status quo bias"—the tendency to maintain the status quo because the perceived negative consequences of change outweigh the potential benefits.[166] Agencies tend to focus on the legal status quo, in which issuance of a court order results in direct access to communications or data. [167] That status quo is threatened if new communication technology does not provide a technical means for complying with the court order. A new and different perspective, emphasized here, is to focus on the positive effects computing and communications technologies have on agencies' surveillance capabilities today. This technology, as addressed above, actually benefits investigatory agencies significantly.

In addition to behavioral economic theory, there are also institutional explanations for the agency focus on decreased surveil-

[163] Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 Geo. Wash. L. Rev. 1306, 1353-1354 (2004).

[164] Daniel Kahnemann et al., *Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias*, 5 J. Econ. Persp. 193, 199-203 (1991). This theory was penned by Daniel Kahneman, who received the Nobel Prize for his work on loss aversion in collaboration with Amos Tversky.

[165] *Id.* at 194–97.

[166] *Id.* at 197-99.

[167] For an earlier version of this discussion of the status quo, *see* Peter P. Swire, *The Administration Response to the Challenges of Protecting Privacy,* (Jan. 8, 2000) (unpublished article), http://www.peterswire.net/stanford7.doc.

lance capability. Certain divisions within government agencies face new obstacles to traditional wiretap techniques. These obstacles pose a threat to that specific division's influence or ability to do its job. Divisions that are affected in this manner have an incentive to object to changing capabilities, and do so by demanding new legal authority or funding. Meanwhile, new surveillance capabilities may be developed within entirely different divisions 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 divisions that face obstacles in the evolving surveillance landscape.

A simple hypothetical can assist the reader in deciding between the "going dark" and "golden age of surveillance" perspectives. Suppose agencies can choose between a 1990-era surveillance package and a 2011-era surveillance package. The first package includes wiretap authority as it existed pre-encryption, but lacks the new techniques for location tracking, confederate identification, access to new databases, and data mining. The second package would match current capabilities: some encryption-related obstacles, but increased levels of wiretaps, as well as new surveillance capabilities. The second 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. These new tools are used far more frequently than wiretaps and provide granular data to assist investigators in both domestic and international investigations.

In conclusion, the 2011-era package is far preferable for investigatory agencies to the 1990-era package. We are indeed living in a golden age of surveillance, in which the agencies greatly benefit from new computing and communications technology. Arguments highlighting the deprivation of surveillance capability are therefore unconvincing. As discussed above, strong encryption is vital to overall cybersecurity and limiting its use leads to the least trusted country problem. The partial degradation of one law enforcement tool should not become the basis for undermining other vital security 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 today, at least some portions of Chinese and Indian industry benefit from limits on strong encryption. This Part 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 domestic trade concerns.

1. U.S. encryption and trade policy in the 1990s

During the 1990s, U.S. software and computing companies led the expansion of the Internet. Microsoft, Oracle and Sun Microsystems pioneered the global software market, Intel and Cisco led the way on microprocessors and routers, and IBM and others were prominent service providers. Export controls on encryption presented a threat to these companies. Foreign competitors were able to sell strong encryption free of restrictions, and the success of these competitors in encryption could be an entering wedge for even broader success for non-U.S. companies. As a result, U.S.-based companies increasingly considered moving production abroad, both to circumvent encryption controls and to compete effectively. This harm to U.S. industry, together with the futility of restricting access to strong encryption, attracted significant political support for strong encryption.

Over time, a more subtle policy issue garnered attention. The U.S. military and other government entities wanted easy access to the most sophisticated encryption available for use in their own systems. Shipping production of encryption overseas could threaten the security of those systems. The Pentagon over time thus shifted from the perspective of the NSA, which favored limits on encryption export, to the perspective that a robust U.S. encryption industry would benefit the nation.[168]

2. China's current trade policy

In contrast with the detailed published history of U.S. encryption events of the 1990s, less is known about the possible trade policy motivations underlying China's current encryption policy. The policy, however, appears broadly consistent with the view that China favors its own nascent encryption industry.

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.[169] Foreign companies wishing to conduct business in China, therefore, must consider the risks that their cutting-edge

[168] This discussion draws on Swire's experience in government during this period.

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 its 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, the nation has a greater chance of obtaining a large share of the global encryption market. Current Chinese strategy may thus 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.[170] 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. This undermines a basic principle of intellectual property protection, to provide incentives for new innovation. Third, the mandate to use only Chinese-produced encryption violates the norms and possibly the rules of international trade rules ensuring fair competition in government contracts.[171] 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 U.S., for example, such subsidies can be the basis for countervailing duties and other trade

[169] *See* James McGregor, *China's Drive for "Indigenous Innovation": A Web of Industrial Policies* (2009), at 15, http://www.apcoworldwide.com/content/PDFs/Chinas_Drive_for_Indigenous_Innovation.pdf (providing a comprehensive overview of these policies).

[170] SuYuan An & Brian Peck, *China's Indigenous Innovation Policy in the Context of its WTO Obligations and Commitment*, 42 Geo. J. Int'l L. 375 (2011).

[171] *See* Christopher S. Gibson, *Globalization and the Technology Standards Game: Balancing Concerns of Protectionism and Intellectual Property in International Standards*, Suffolk University Law School Faculty Publications 43 (2007), *available at* http://lsr.nellco.org/suffolk_fp/43/ ("some of the Chinese government measures used to promote WAPI, including its initial (but later suspended) mandate that all wireless devices sold or imported into China must be WAPI compliant, can be viewed as protectionist, raising concerns in relation to WTO obligations.").

sanctions.[172] The U.S. and other countries continue to object to China's Policy, though minor changes have resulted from ongoing negotiations.

Having non-standard cryptography acts as a trade barrier, as illustrated by China treating the ZuC LTE standard as mandatory when global standards organizations treat it as optional.[173] The mandatory use of ZuC in China means that LTE equipment produced in the rest of the world will not be considered compliant with Chinese requirements, thereby blocking use of standard technology.

Even more compelling than international trade issues are the cybersecurity and policy implications of China's approach to encryption. 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."[174] 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 require installation of 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; many users, however, 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 and critical infrastructure. Hardware, however, is typically much more difficult to patch than software. Though

[172] *See* Agreement on Subsidies and Countervailing Measures, Apr. 15, 1994, *available at* http://www.wto.org/english/docs_e/legal_e/24-scm.pdf (last visited Aug. 17, 2011).

[173] *See supra* notes 88-91 and accompanying text (describing ZuC algorithms).

[174] Ferguson, *supra* note 25, at 13.

software patches involve cumbersome downloads, actual physical replacement may be required for 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 developed the AES cipher.[175] Early weaknesses have 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 could use 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 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. A related concern is that the use of non-standard encryption will produce a specific opportunity for the Chinese government to tap into a wide range of encrypted communications. Communications using global standards will be lawful until they are received in China; at that point, the practice may become to decrypt the communication in order to re-encrypt it with a Chinese algorithm. This decryption and re-encryption creates the opportunity for systematic government access at the time that the communication is in plaintext.

[175] AES stands for Advanced Encryption Standard, a symmetrical-key encryption system that was adopted as the federal standard in 2001. *See* Nat'l Inst. of Standards & Tech., Fed. Info. Processing Standards Publ'n No. 197, Announcing the Advanced Encryption Standard (AES) (2001), *available at* http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf (outlining the specifications for the Advanced Encryption Standard).

Chinese insistence on employing lightly tested cryptosystems thus faces strong objections on both trade and cybersecurity grounds. This Article 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 skilled programmer in the field creates a cryptosystem, peer review 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's current trade policy

The international trade situation in India today is similar in important respects to that in the U.S. during the 1990s. India's business process outsourcing (BPO) sector now accounts for over 6% of India's GDP.[176] 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 the BPO sector. Suppose, for example, that health insurance companies or hospitals in the U.S. 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. U.S. 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 respective countries. This scenario 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.

[176] *See* Press Release, NASSCOM, IT-BPO industry: Strong growth with focus on transformation and enhanced value proposition (Feb. 2, 2011), *available at* http://www.nasscom.in/node/60499.

Current standards require the EHR technology to employ strong encryption.[177]

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.[178] In the U.S., the Gramm-Leach-Bliley Safeguards rule similarly requires the implementation of risk-based security measures for financial institutions.[179] Given the relatively low cost and high strength of commercial encryption today, regulators and BPO competitors have a strong argument that weak encryption in India violates such security laws.

Other India trade policy concerns relate to technology transfer. Similar to China and other nations, India would like to foster technology transfer and training of its domestic workforce up 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 regards to the telecommunications and computing sector. Unlike China, India has not pressed for the production and export of domestic encryption. India instead may be leaning towards implementing import controls on encryption. The controls would potentially require an import license for incoming encryption products, certifying compliance with India's encryption laws and upholding the national security agencies' desire to limit effective encryption.

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

[177] 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. 45 C.F.R. § 170.302 (2012).

[178] In April 2011 India adopted new data privacy rules with which it seeks, in part, to meet the "adequacy" requirements of existing E.U. data protection laws. However, no privacy policy can be considered "adequate" if it is implemented in a thoroughly insecure manner—i.e. without encryption, or with weak encryption. For a basic overview of India's new privacy laws see Peter Brown, *New Indian Privacy Law Impacts U.S. Companies*, Bakerlaw.com, (Aug. 3, 2011), http://www.bakerlaw.com/alerts/new-indian-privacy-law-impacts-us-companies-8-3-2011.

[179] 15 U.S.C. § 6801(b) (2012).

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 used during the U.S. crypto debates in the 1990s. Strong encryption is even more widely accessible today than it was in the 1990s. Once again, malicious actors would have access to effective encryption while legitimate actors would be trapped with weak cybersecurity.

D. Summary of Trade Policy Considerations

The strongest cryptosystems today are the subject of constant and sophisticated testing by an international community of experts. National encryption policies that depart from international standards are likely to undermine security infrastructure and hamper both domestic and foreign business growth and innovation. To assist domestic industry, countries may be tempted to rely on homegrown encryption; however, the discussion above illustrates that this approach violates both international trade standards and the objectives of cybersecurity.

CONCLUSION

In essence, this Article advocates for the position adopted by the United States at the end of the crypto wars of the 1990s—strong cryptography should be deployed widely because it is essential for the Internet and computing. The logic of this position was so overwhelming that it remained firmly in place after September 11, 2001, even as the United States adopted other measures to provide new powers for law enforcement and national security agencies.

The simplest case for encryption is that it is too risky for Alice to communicate to Bob over an insecure channel such as the Internet when anyone in the middle can listen in. Millions of insecure nodes lie in between Alice and Bob on the Internet, any one of which can copy the information and send it to a malicious party. Because we use the Internet today for a huge and growing number of important transactions—banking, medical records, and government activities—we need strong encryption in order to protect those transactions.

The Internet, in turn, is only one example of how modern computing relies on encryption and other aspects of cryptography. The technologies discussed in this Article perform essential tasks, such as preventing unauthorized people from accessing our information, assuring that the information is the same as originally sent, and authenticating the source of the information. Government rules that threaten these tasks threaten computing generally. Vigorous and public peer review of cryptographic protocols, notably through the international standards process, is the best way to assure this strong security.

This Article has explained how limits on cryptography operate as backdoors—as intentional flaws in cybersecurity. Susan Landau also highlights this concern in her book *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*. The Clipper chip and key escrow proposals of the 1990s were examples of government-designed vulnerabilities, and their profound flaws should inform the new global encryption debates.

In a networked world, flaws in one nation affect other nations. The nations with limits on cryptography become security holes in the network—bits to, from, or through those nations are subject to compromise.[180] For nations as large as India and China, numbering well over two billion people, the scale of the security holes would affect the overall trustworthiness of the Internet and of networked computing. In addition, the "least trusted country" argument illustrates what happens if multiple countries insist on imposing strict limits—there is a race to the bottom where the level of trust is only as high as the least trusted country.

Law enforcement and national security agencies will indeed face new obstacles from new technologies, and the authors plan in future research to analyze how international procedures for court orders and other lawful process should evolve with changing technology. The major advantages to these agencies resulting from new technology, however, put their modest losses from encryption into a clearer context.

The discussion in this Article has brought together, for the first time since the end of the U.S. crypto wars, the reasons why effective cryptography is essential to modern computing. Those reasons are even more compelling in our globalized setting today, where security flaws in one country have such dramatic effects on other countries. Cybersecurity is a central challenge of our age, and effective cryptography should play a central role in achieving that security.

[180] As a variation, other countries could reduce their inter-operability with the country that limits effective cryptography. Such limits on inter-operability can reduce the security loss. The loss instead would be reduced gains in trade—a reduction in all of the benefits of being connected to the other country.