SURVEILLANCE'S SLIPPERY SLOPE: USING ENCRYPTION TO RECAPTURE PRIVACY RIGHTS

DANIEL J. SHERWINTER[*]

INTRODUCTION

> "Is freedom inversely related to the efficiency of the available means of surveillance? If so, we have much to fear."[1]

The digital revolution happened very quickly. Only 20 years ago, fewer than 10 percent of American households had computers.[2] However, by as early as 1993, the number of American households with computers had already risen to almost 25%.[3] At the same time, the Internet was quickly growing in popularity. Tim Berners-Lee debuted the World Wide Web on August 6, 1991, and within five years, most publicly traded companies had websites.[4] This was the dawn of a new information age.

Now, it seems that Internet access points are everywhere. In addition to having access to the Internet at home and at the office, it is becoming increasingly rare to find a coffee shop, university, or library which does not provide Internet access to its patrons. This global infor-

[*] Daniel Sherwinter is a J.D. candidate at the University of Colorado (2007), Executive Editor of the Journal on Telecommunications and High Technology Law, and recipient of the Thomas Schatzel Intellectual Property Law Scholarship. He will be joining Townsend & Townsend & Crew as a patent prosecution associate in their Denver office in Fall 2007. He thanks Professor Phil Weiser, Professor Paul Ohm, Professor Doug Sicker, Cynthia Sweet, Travis Litman, and James Crowe for taking their precious time to provide extremely helpful feedback and ideas. He would like to dedicate this publication to his wife, Karli, for her tireless help and support through the writing process, and his new baby daughter, Kayla Tamar, for her tiring support just prior to sending this paper to print.

[1] JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY 4 (1996).

[2] U.S. Census Bureau, Current Population Survey 1984 (In 1984, 8.2% of American households had at least one computer.).

[3] U.S. Census Bureau, Current Population Survey 1993 (In 1993, 22.6% of American households had at least one computer.).

[4] *See* Wikipedia, History of the World Wide Web, http://en.wikipedia.org/wiki/History_of_the_World_Wide_Web (last visited Feb. 4, 2007).

mation network lets people shop for goods and services, trade commodities on world markets, find information on myriad subjects, and stay in communication.

Further, this same information provides tremendous new opportunities for law enforcement. Surveillance through the interception of communications is an important law enforcement tool. Tapping[5] a criminal's phone conversation may reveal details of a pending heist, admissions of guilt, associations with other criminals, and other potentially incriminating evidence. But the Internet can provide the same information, plus much more, including a criminal's passwords, search patterns, and spending patterns.[6] Law enforcement can use these new capabilities to improve the security[7] of the nation.

Historically, surveillance laws have attempted a careful balance between the security needs of the nation against the privacy rights of its citizens. Recently, however, despite an erosion of privacy rights, the trend in surveillance has favored security over privacy. This trend has included an expansion of CALEA[8] to cover certain broadband communications, and an application of the USA PATRIOT Act[9] to justify the domestic surveillance of Americans. The question, then, is what the public can do to preserve their right to privacy in the face of this erosive trend.

One promising solution is the ubiquitous adoption of strong encryption. Currently, most Internet users fail to adequately encrypt their online communications. Using strong encryption, however, can render online communication virtually undecipherable to unauthorized eavesdroppers. Therefore, even though the Internet gives law enforcement agencies added surveillance power, individuals can limit that power through encryption. In that way, the ubiquitous usage of strong encryption can help restore the balance between privacy and security.

This comment begins in Part I with an overview of the right to privacy and its importance to American society. Part II presents the development of the framework of Federal surveillance laws, ending with the

[5] In this paper, "tapping" or "wire tapping" refers to eavesdropping on a phone call through some electronic means.

[6] Some may argue at this point that there is so much information on the Internet that it is increasingly difficult to separate out the useful information. Digital information, however, better lends itself to filtering, sorting, searching, comparing, and other invaluable data processing techniques.

[7] Throughout this paper, I have used the term "security" to refer to public, or national security (not computer security, or physical security against personal crimes).

[8] Communications Assistance for Law Enforcement Act (CALEA) of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 18 U.S.C. and 47 U.S.C.).

[9] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001) [hereinafter Patriot Act].

recent trend away from the preservation of privacy rights. Section III provides a background to encryption technology and its importance in preserving communication privacy. Section IV discusses the government's failure with and retreat from encryption regulation, which has set the stage for worldwide e-commerce and the free flow of information. The background from Sections II through IV frames a discussion in Section V on the ability of encryption to defeat law enforcement's surveillance regime under the expanded CALEA Order. Given the inefficacy of Internet surveillance in the face of encryption, Section VI will examine other options and considerations for law enforcement. Finally, Section VII will conclude the comment.

I. THE RIGHT TO PRIVACY

The right to privacy is nowhere in the text of the Constitution. However, the history of Constitutional jurisprudence has demonstrated the accepted belief that the right to privacy inheres within the Constitution's language, and that privacy must be protected both procedurally and substantively. In 1890, future Justices Warren and Brandeis defined four types of privacy torts that are based on a substantive right to privacy.[10] The Supreme Court upheld the substantive right to privacy in the seminal case, *Griswold v. Connecticut*.[11] In that case, Justice Douglas claimed that the Bill of Rights creates a penumbra of inherent rights, including the right to privacy. Consenting opinions in *Griswold* also found the right to privacy inherent in the Ninth Amendment's un-enumerated rights[12] and the Fourteenth Amendment's notion of substantive due process.[13] In addition to the substantive right, there is also a procedural privacy right inherent in the Fourth Amendment's prohibition against illegal search and seizure.

While these privacy rights inhere in the Constitution,[14] they are not considered fundamental rights to American society. Even though privacy preservation is extremely important, "privacy is not an absolute good because it imposes real costs on society."[15] Thus, lawmakers must always weigh privacy against competing interests, like national security. This is a particularly difficult balance–some believe that privacy is mean-

[10] Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). *Cf.* Jeffrey Cole, *My Afternoon with Alex: An Interview with Judge Kozinski*, 30 LITIGATION 12 (Summer 2004) (Justice Kozinsky of the Ninth Circuit said about the Warren and Brandeis article, "Seldom had I seen so much made out of so very little with quite so much zest. . . . [It] was the legal equivalent of a soufflé—all air, no substance, tastes great.").

[11] Griswold v. Connecticut, 381 U.S. 479 (1965).

[12] *Id.* at 487 (Goldberg, J., concurring).

[13] *Id.* at 500 (Harlan, J. and White, J., concurring).

[14] *See id.;* Brandeis & Warren, *supra* note 10, at 193.

[15] U.S. West v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999).

ingless in an insecure country, while others believe that a country without privacy is not worth securing. That balance between privacy and security frames much of the debate surrounding both surveillance and encryption.

Surveillance can be very important to national security, but it can also threaten individual privacy. After all, the purpose of surveillance is to reveal that which an individual intends to conceal. If the FBI uses sophisticated thermal imaging to watch a person in her home without a warrant, they arguably infringe her substantive right to be left alone in her home, while simultaneously performing a procedurally illegal search.[16] The FBI may contend, however, that without surveillance, more criminal activity would threaten the safety of Americans. Similarly, encryption provides a means for substantive privacy through anonymous (or pseudonymous) communication, and a means for procedural privacy through secure data transmission. As before, the FBI may argue that, by using encryption, more criminals can plan illegal behavior without getting caught, thereby harming society.

In the end, absolute security requires totalitarianism, but total privacy creates anarchy. Therefore, regulations on surveillance and encryption must balance these competing privacy and security rights. When regulators fail, people must be willing to take control of their rights to restore the balance. The current failure to maintain that balance is the focus of Parts II and III.

II. FEDERAL ELECTRONIC SURVEILLANCE REGULATIONS

> Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate . . . the constitutional rights of each of us as potential recipients of encryption's bounty.[17]

The Internet has forever changed the way we communicate. In the past, people communicated over long distances through the mail. If they desired to deter people from reading their letters in transit, they sealed the letters in an envelope. The advent and spread of electronic commu-

[16] The substantive privacy right in question here may be "intrusion upon seclusion," one of four torts formulated by Brandeis and Warren in *The Right to Privacy*, *supra* note 10. *See also*, Kyllo v. United States, 533 U.S. 27 (2001) (involving thermal imaging surveillance).

[17] Lee Tien, *Doors, Envelopes, and Encryption: The Uncertain Role of Precautions in Fourth Amendment Law*, 54 DEPAUL L. REV. 873, 903 (2005) (quoting Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1146, *withdrawn by* 192 F.3d 1308, 1309 (9th Cir. 1999)).

nications, however, came with no easy equivalent, and communications traveled unprotected over publicly accessible wires and airwaves. The rise of the Internet and more powerful computing created a massive increase in the amount of information traversing those media. The newly-enabled content now consisted of both conversations and data (i.e., packets of 1's and 0's containing the details of everything from financial transactions to strategic plans to trade secrets). As more information traveled the globe, wiretapping became critical to law enforcement.[18] However, this new tool also brought new responsibility. Now, with secret remote surveillance, the government could avoid the "knock and announce" types of notice requirements critical to Fourth Amendment protections from illegal searches and seizures.[19]

A. Historic Federal Surveillance Regulation Balanced Privacy and Security

> "Our government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the government becomes a law-breaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy."[20]

The drafters of the Fourth Amendment saw illegal searches as involving physical trespass onto property. When *Olmstead*, the first major wiretapping case, reached the Supreme Court in 1928,[21] the majority seemed to rely on that conception of "searching." The majority held that communications traveling via the phone lines (or presumably the airwaves) were essentially public. As such, the Court held that eavesdropping was not a violation of Constitutional liberties. Government abuses of this newfound power began to see their way to the Supreme Court in the late 1960's,[22] prompting the Supreme Court to reverse *Olmstead*. In 1968, Congress attempted to balance privacy rights against the needs of law enforcement by passing a set of Federal wiretap provisions. Congress adopted this new act as Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[23] Under these provisions, law enforcement

[18] *See, e.g.*, Berger v. New York, 388 U.S. 41, 60-62 (1967) (stating that "electronic eavesdropping is a most important technique of law enforcement").

[19] Richards v. Wisconsin, 520 U.S. 385, 395 (1997).

[20] Olmstead v. United States, 277 U.S. 438, 485 (1928) (Brandeis, J., dissenting).

[21] *Id.*

[22] In 1967, the Supreme Court heard two seminal cases in this area: Berger v. New York, 388 U.S. 41 (1967), and Katz v. United States, 389 U.S. 347 (1967). These cases effectively overturned *Olmstead.*

[23] 18 U.S.C. § 2510 (2005). This section is also known as "Title III" or the "Federal

could lawfully intercept any wire or oral communication, but only within strict guidelines. For example, a court order permitting the surveillance would only be issued with probable cause,[24] as a last resort when other surveillance was ineffective,[25] and only to combat one of 26 specific crimes.[26] Further, even with a court order, wiretapping had to be accomplished with minimal invasions of benign conversations,[27] and notice had to be given to the subject of the surveillance upon completion of surveillance.[28] The Federal wiretap statute was seemingly a successful compromise between privacy and public safety.

Unfortunately, the compromise did not last long. Since that time, and with each subsequent piece of legislation, the trend has been towards an erosion of privacy rights. The dire results of this trend have become increasingly apparent recently with the use of the Patriot Act to spy on Americans and the expansion of CALEA to allow surveillance of broadband communications.

B. From FISA to the Patriot Act – A Procedural Erosion of Privacy Rights

> "The PATRIOT Act addressed only one side of this [privacy-security] equation, making government access easier without counterbalancing privacy improvements. Now is the time for Congress to finish the job and address the privacy side of the equation."[29]

Just ten years after the passage of the Federal Wiretap Act, Congress passed the Foreign Intelligence Surveillance Act (FISA) of 1978. FISA attempted to make wiretapping easier in national security-related cases[30] by weakening both the probable cause[31] and notice[32] requirements for wiretapping agents of foreign powers. To preserve the privacy of Americans, however, Congress required that surveillance orders only

Wiretap Act".

[24] § 2518(3).

[25] *Id.*

[26] § 2516(2).

[27] § 2518(5) (providing the minimization requirement).

[28] § 2518(8)(d).

[29] *Oversight Hearing on Implementation of The USA PATRIOT Act: Sections of The Act That Address Crime, Terrorism, and The Age of Technology: Hearing before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 109th Cong. (2005) (statement of James X. Dempsey, Executive Director of the Center for Democracy & Technology) *available at* http://www.cdt.org/testimony/20050421dempsey.pdf.

[30] 50 U.S.C. §§ 1801-11 (2005).

[31] § 1805(a)(3)(A) (retaining a probable cause requirement but commission of a crime is no longer considered probable cause on its own).

[32] § 1806(c) (removing the notice requirement when law enforcement decides not to use the information acquired through the surveillance in a criminal proceeding).

be given under FISA when "the purpose of the surveillance [was] to obtain foreign intelligence information."[33] This essentially restricted the use of FISA surveillance orders to foreign counterintelligence operations.

Still, the application of FISA and its predecessors began to reveal a trend away from the privacy protections seemingly intended by those earlier laws. One example of this is that while Title III had originally listed only 26 crimes in 1968 as valid reasons for obtaining a wiretap, Congress increased the list to 95 crimes by 1996.[34] Other examples were evident in the courts' granting increasing numbers of wiretap orders with longer durations,[35] holding that wiretaps may be permitted even when not only used "as a last resort,"[36] exhibiting an extremely lax approach to the "minimization requirement,"[37] and consistently rejecting post hoc challenges to surveillance authority.[38] The shift away from privacy-protective surveillance limitations continued steadily through the 1980's and 1990's.

On September 11, 2001, however, domestic terrorist attacks suddenly changed the American concept of war, and suddenly perched privacy on the precipice of a slippery slope. Overnight, domestic terrorism forced Americans to rethink personal privacy in light of heightened national security concerns. In this environment of public fear, President Bush and Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act, or "Patriot Act") of 2001.[39] Much of the Patriot Act extended FISA to aid in the domestic war on terror by removing some of its remaining privacy-protective hurdles to domestic surveillance.[40] For example, while FISA initially required identification of the target or place of a wiretap, § 206 of the Patriot Act amended FISA to

[33] § 1804(a)(7)(B).

[34] James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 75 (1997).

[35] Administrative Office of the United States Courts, *2002 Wiretap Report*, Table 5, http://www.uscourts.gov/wiretap02/table5-02.pdf. Since 1986, there have been almost no denials of requests for wiretap orders, and the number of wiretaps requested has consistently increased. In 2002, for example, there were 1,273 orders for which wiretaps were actually installed, costing a total of almost $70 million, and resulting in 493 convictions. *Id. See also* Dempsey, *supra* note 34, at 75 (the quantity of wiretaps was 564 in 1980 and 1,149 in 1996).

[36] United States v. Garcia, 785 F.2d 214, 223 (8th Cir. 1986) (weakening the "necessity" requirement, but not completely removing it).

[37] *See generally*, Dempsey, *supra* note 34, at 75-78.

[38] *Id.*

[39] *See* Patriot Act, 115 Stat. 272.

[40] *E.g.*, Patriot Act § 218, 115 Stat. 272 (amending FISA to allow surveillance where "a significant purpose," rather than "the purpose" is to gather foreign intelligence. This allows surveillance in a much broader group of criminal cases which formerly fell under law with more stringent privacy protections, like the Wiretap Act).

only require that identification "if known."[41]

Though many feared the privacy implications of the Patriot Act, the threat to privacy stretched farther than most predicted. On December 16, 2005, the New York Times reported that, since September 11, President Bush, in the name of national security, had authorized the surveillance of possibly thousands of people within the United States without a court order.[42] Bush admitted to signing a secret executive order in 2002 which "authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying. . . ."[43]

Though FISA's initial language limited its reach to agents of foreign powers, the Bush administration argued that its amended form allowed for warrant-free domestic surveillance as well. The administration put forth the following legal justification:[44] first, FISA requires a court order for all domestic surveillance, but allows the President to bypass that requirement when authorized by a different statute;[45] second, the Authorization for Use of Military Force Against Iraq, passed in 2002, allows the President to authorize force (even domestically) to combat terrorism;[46] third, "throughout history, signals intelligence [i.e. surveillance] has formed a critical part of waging war";[47] fourth, the Authorization for Use of Military Force is a different statute which allows the President to bypass the court order requirement of FISA; and finally, the President can, therefore, lawfully authorize domestic surveillance without a court order. Thus, according to the Bush administration, U.S. surveillance law now permits domestic surveillance without a court order and without notice.

Whether or not this legal analysis proves to be upheld, the logistical hurdles of surveillance laws have certainly lessened in the past few decades. These procedural changes have tilted the balance away from privacy protection in the name of national security. In addition, attempts to adapt surveillance laws to changes in technology have further eroded

[41] 50 U.S.C. § 1805(c)(1)(A) (2000).

[42] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html.

[43] *Id.*

[44] David Johnston & Neil A. Lewis, *Defending Spy Program, Administration Cites Law*, N.Y. TIMES, Dec. 23, 2005, at A20, *available at* http://www.nytimes.com/2005/12/23/politics/23court.html.

[45] *See* §§ 1801-11.

[46] Authorization for Use of Military Force Against Iraq Resolution of 2002, Pub. L. No. 107-243, 107th Cong. (Oct. 16, 2002).

[47] Johnston & Lewis, *supra* note 44 (quoting a letter justifying the President's actions to Congress, signed by William E. Moschella, assistant attorney general for Congressional affairs).

privacy rights.

C. From ECPA to the CALEA Order – A Technological Erosion of Privacy Rights

> "[The FCC has] plainly overreached their authority in requiring Internet providers to design systems that make surveillance of the public easier and we are confident that the courts will agree. . . .The FCC needs to call a timeout until it knows what it wants, and seriously reconsider whether it has the authority to demand it."[48]

In the 1980's, shortly after the Federal Wiretap Act passed, the communications arena began to change. Wireless communication was becoming prevalent and large amounts of non-voice data were being transmitted between computers. This created an opportunity for more surveillance, and a need for more privacy protection. In 1986, Congress expanded surveillance laws into those new realms with the Electronic Communications Privacy Act (ECPA).[49] Title I of the ECPA amends the Federal Wiretap Act to cover digitized communications, and Title II covers stored communications (like e-mail) and call-related information beyond the content of the communication.[50] Congress justified the ECPA on grounds that surveillance technology was expanding faster than privacy protection, and that encouragement of technological innovation must not cost the public its rights.[51]

In the early 1990's, in the midst of increasing electronic surveillance, some law enforcement agencies noticed changes that made surveillance less effective.[52] These changes were both logistical and technological: More competition in telecommunications meant more choices and the option to use multiple providers; and technologies like digital circuit switches, call forwarding, and speed dial sometimes obscured the

[48] Electronic Frontier Found., *FCC Urged to Suspend New Internet Wiretap Rules*, EFFECTOR, Nov. 25, 2005, http://www.eff.org/effector/18/41.php (quoting EFF Senior Staff Attorney Lee Tien).

[49] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat 1848. (codified in scattered sections of 18 U.S.C.).

[50] 18 U.S.C. §§ 3121-27 (1996) (covering call information, including phone numbers, dates, and times of calls; as well as the use of devices which track phone numbers, like pen registers (which track outgoing calls) and trap and trace devices (which track incoming calls)).

[51] Pub. L. No. 99-508, H.R. Rep. No. 99-647, at 17-19 (1986).

[52] *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375: Hearing Before the Subcomm. on Tech. and the Law of the S. Comm. on the Judiciary and Before the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 103rd Cong. 5-6 (1994) (testimony of Louis J. Freeh, Director, Central Intelligence Agency).

origin or destination of a call.[53] In 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA), "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes."[54] In other words, CALEA required telecommunications carriers to engineer their facilities and services to allow easy access for law enforcement surveillance equipment.[55]

A number of organizations, including the Electronic Frontier Foundation (EFF), the Center for Democracy and Technology (CDT), the Electronic Privacy Information Center (EPIC), and the American Civil Liberties Union (ACLU), actively challenged CALEA for its potential negative repercussions to privacy.[56] Implementing CALEA required many decisions regarding specific obligations and technologies, and many organizations wrote comments and press releases to bolster the privacy-protective side of the debate. One specific limit to the privacy-erosive potential of CALEA was its limitation to traditional voice communications, as opposed to "information services" like Internet communications.[57]

In today's world, however, voice communications are no longer restricted to the Public Switched Telephone Network (PSTN). To be comprehensive, surveillance cannot remain restricted to traditional types of phone calls. Telephone-like conversations now occur through multiple channels, including Voice-Over-Internet-Protocol (VoIP), instant messaging (IM), e-mail, and text messaging. Thus, in August 2005, the Federal Communications Commission (FCC) adopted an Order extending the coverage of CALEA to "facilities-based broadband Internet access providers and providers of interconnected VoIP service."[58]

Issues with the Order have incited vehement protests from many organizations.[59] First, changing technology cannot automatically justify sacrificing individual privacy rights.[60] Second, The Order's 18-month

[53] *Id.* at 121.

[54] *See* CALEA, 108 Stat. 4279.

[55] 47 U.S.C. § 1002 (2000).

[56] *See, e.g.*, USTA v. FCC, 227 F.3d 450, 452-53 (D.C. Cir. 2000). The various organizations list many press releases, statements, and other comments available on their respective websites.

[57] *See* CALEA § 103(b)(2)(A).

[58] Communications Assistance for Law Enforcement Act and Broadband Access and Services, *First Report & Order & Further Notice of Proposed Rulemaking*, 20 FCC Rcd. 14,989 (2005) [hereinafter Order].

[59] *E.g.*, Comments of EPIC, EFF and ACLU, to the *Notice of Proposed Rulemaking & Dedclaratory Ruling* in Communications Assistance for Law Enforcement Act, CC Dkt. No. 97-213 (Dec. 14, 1998) (challenging the DOJ/FBI "punchlist" proposal), *available at* http://www.epic.org/privacy/wiretap/calea/comments_12_98.html.

[60] Though many argue that CALEA has inherent limitations to potential negative privacy implications, those arguments are unconvincing. The first arguable limitation is that

compliance deadline will saddle many universities, libraries, airports, Internet service providers, and municipalities with huge compliance burdens.[61] Third, adding back doors to more networks adds potentially-vulnerable access points for hackers.[62] Finally, many have argued that the FCC does not even have jurisdiction to issue this Order, stating: "The debate over the scope of CALEA was fought in Congress during the debate and passage of the CALEA statute, and it was determine [sic] that CALEA would not extend to the Internet. Frankly, it is inappropriate for a regulatory body to reinterpret the clear intent of Congress."[63]

History suggests that the initial intention of the surveillance laws was to carefully limit the government's power to surveil the public in order to protect the public's right to privacy. Fears of national security threats, however, have justified an ever-waning restriction on the government's power to infringe those rights. The recent publicity of executive surveillance orders and the CALEA Order highlights the reality of surveillance law's slippery slope. We must challenge the laws which threaten the delicate balance between privacy and security before it is too late. In the digital world, strong encryption technology may be an effective privacy-protective option to help restore that balance.

various pieces of surveillance legislation require government and law enforcement to obtain a court order before performing surveillance. However, news of the President's secretive authorization of domestic surveillance (*see supra* Part II.B) tends to belie these claims. Also, the trend of surveillance laws reveals the gradual disappearance of those logistical hurdles, showing that society cannot rely on them for privacy protection. Second, the Order does not expand CALEA to reach all types of broadband communication. For example, while the Order reaches managed VoIP services like Vonage, e-mail and peer-to-peer VoIP (like Free World Dialup) probably are not required to comply. However, there are two problems with relying on that statement: (1) It is still unclear exactly who must comply and in what way; and (2) just as the original CALEA language specifically excluded information services like Internet service from compliance, this Order may mark one of a series of expansions to CALEA's reach over time.

[61] Sam Dillon & Stephen Labaton, *Colleges Oppose Call to Upgrade Online Systems*, N.Y. TIMES, Oct. 23, 2005, at A1 (estimating compliance costs of over $7 billion for universities alone).

[62] *See, e.g.*, Electronic Frontier Foundation, Communications Assistance for Law Enforcement Act (CALEA), http://www.eff.org/Privacy/Surveillance/CALEA/ (last visited Feb. 4, 2007) ("While law enforcement's efforts to hijack the tech market are disturbing, EFF is also concerned that making the Internet CALEA-compliant might backfire: many of the technologies currently used to create wiretap-friendly computer networks make the people on those networks more pregnable to attackers who want to steal their data or personal information.").

[63] Press Release, Center for Democracy and Technology, Public Interest, Business Groups Unite to Challenge FCC Wiretapping Rules (October 25, 2005) (quoting Jeff Pulver, chairman and CEO of Pulver.com), *available at* http://www.cdt.org/press/20051025calearelease.pdf.

III. OVERVIEW OF ENCRYPTION TECHNOLOGY[64]

> "[E]ncryption technologies are the most important technological breakthrough in the last one thousand years."[65]

Law enforcement continually demands the ability to conduct surveillance with the latest technologies. The obvious reason for these demands is that people are increasingly using the latest types of communications to plan everything from dinner parties to corporate takeovers to terrorist attacks. As people communicate greater quantities of more important information, the rewards for intercepting that information grow. Encryption is a critical step in keeping electronic information secure from surreptitious interception by governments, business competitors, criminals, and others.[66] This is of critical importance as governments, companies, individuals, and others are increasingly in possession of data requiring protection. Moreover, no one wants their trade secrets, employee information, customer information, or other private data compromised.

A. Brief History of Encryption

> "History is punctuated with codes. They have decided the outcomes of battles and led to the deaths of kings and queens."[67]

There are three main categories of encryption methods: Classical, rotary, and digital.[68] The earliest category, classical encryption, consisted of substitution and transposition algorithms. Complex numerological coding of letters was used as far back as the scribes of Susa and Babylon in the 8th century BCE.[69] Ancient codes and cryptograms were primarily used for mysticism and haruspicy.[70] More recently, Julius

[64] For a more comprehensive overview of encryption-related technology, policy, law, and history, *see* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE (1996); SIMON SINGH, THE CODE BOOK (1999).

[65] LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 35 (1999).

[66] Aaron Tan, *Ellison: Encryption is Key to Data Protection*, CNET, Sept. 23, 2005, *available at* http://www.nytimes.com/cnet/CNET_2100-7355_3-5879101.html ("[N]o company would want to face the situation where storage tapes containing unencrypted customer credit card information are lost. And as . . . businesses switch from traditional phone networks to converged voice-data networks, security will become even more crucial. . . .").

[67] SINGH, *supra* note 64.

[68] Sam Siewert, *Big Iron Lessons, Part 6: The Right Coprocessor Can Help with Encryption*, Aug. 16, 2005, http://www-128.ibm.com/developerworks/power/library/pa-bigiron6/index.html.

[69] GEORGES IFRAH, THE UNIVERSAL HISTORY OF NUMBERS 160-61 (2000).

[70] *Id.*

Caesar is said to have sent military orders using a secret code, whereby each letter of the alphabet was substituted with a letter from a rearranged or shifted alphabet.[71] For example, if Caesar had used the English alphabet and shifted each letter three places, the word "CAT" would become "FDW." This type of encryption is simple to perform by hand, and almost as simple to crack.

The second category, rotary encryption, used mechanical devices to make what were essentially very complex "Caesar" ciphers. For example, in World War II, the Axis powers could preset rotors, buttons, and other mechanisms on a complex device called the Enigma machine. The machine would use those preset values to convert messages to unreadable code. Without having an Enigma machine and knowing the preset code, it was nearly impossible to crack the code. However, the Allied forces eventually got hold of Enigma machines and were able to break the cipher.[72] The result of this cryptographic success was the acknowledgment of the importance of cryptographic research as "vital to [national] security," which, in turn, lead to President Truman's formation of the National Security Agency.[73]

Modern cryptography developed an entire branch of mathematics that uses algorithms to transform data between its readable form (known as plaintext) and a coded, unreadable form (known as ciphertext). As codes get more complicated, so does the associated math. It is no surprise that the NSA is "said to be the largest employer of mathematicians in the United States and perhaps the world."[74] But even the greatest math minds are no match for the processing speed of a computer. With the advent of computers came the potential for solving complex mathematic problems very rapidly, and the third category of encryption—digital encryption.

B. Computers and Strong Encryption

> "The world isn't run by weapons anymore, or energy, or money. It's run by little 1's and 0's, little bits of data. It's all just electrons."[75]

[71] Adam C. Bonin, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL F. 495, 497 (1996).

[72] HERVIE HAUFLER, CODEBREAKERS' VICTORY: HOW THE ALLIED CRYPTOGAPHERS WON WORLD WAR II (2003).

[73] Sam Siewert, *Big Iron Lessons, Part 5: Introduction to Cryptography, from Egypt Through Enigma*, July 26, 2005, http://www-128.ibm.com/developerworks/power/library/pa-bigiron5/.

[74] National Security Agency Central Security Service, Introduction to NSA/CSS, http://www.nsa.gov/about/index.cfm (last visited Feb. 4, 2007).

[75] SNEAKERS (Universal Studios 1992).

Some computers today are able to make trillions of calculations per second.[76] Since encryption mostly involves sets of large mathematical operations, computers are an ideal tool for both encrypting and decrypting data. Suppose that a cryptographic algorithm adds binary "10" (i.e. "00000010"), the "key," to 8-bit ASCII representations of plaintext letters.[77] The result may be as follows:

Plaintext: 'C A T' ➔ 01000011 / 01000001 / 01010100
Add Binary "10": 01000101 / 01000011 / 01010110
Ciphertext Result:01000101 / 01000011 / 01010110 ➔ 'E C V'

Thus, the plaintext "CAT" is passed to the algorithm, and is converted to the unreadable ciphertext "ECV." Most modern encryption methods work in essentially this way – plaintext is converted to unreadable ciphertext via some algorithm which makes use of a key.

There are two typical factors for determining the effectiveness of a key: its secrecy, and its length. Key secrecy, here, refers to how well the key remains hidden. Historically, the key had to be handed off to the recipient in order to decipher the message, creating a weakness in the encryption. Say that A wants to send a message to B in a box. A locks the box and sends it to B. Somehow, A must also send the key, or B cannot open the box (and for the same reasons, A cannot securely send the key). However, what if A sends the locked box, and then B adds her own lock to the box and returns the box to A. Then, A unlocks only his lock, and re-sends it to B. B has now received the box only with her own lock, for which she has the key! In the 1970's, Whitfield Diffie and Martin Hellman devised public-key encryption, an ingenious version of this solution for encryption key exchange.[78] By using a private key and a public key together, the Diffie-Helman algorithm has eliminated the issue of key exchange.

The second traditional issue with encryption keys is their length. Generally, longer keys provide stronger encryption. In the above example, the key is only two bits long. It would take no time to guess the key by trying each of the four possible keys.[79] Thus, the strength of this type of encryption algorithm increases exponentially with the length of the

[76] Stephen Shankland, *IBM Set to Take Supercomputing Crown*, CNET, Nov. 5, 2004, http://news.com.com/2100-1010_3-5439523.html (announcing that IBM's new incarnation of Big Blue can perform 70.7 trillion calculations per second).

[77] The ASCII (American Standard Code for Information Interchange) character set is a standard table of 128 correspondences between characters and 8-bit values. For example, the character 'C' corresponds to the bits '01000011', and the character '#' corresponds to the bits '00100011'. This example assumes that the plaintext data is encoded using the ASCII character set. For a full ASCII character set table, *see* http://ostermiller.org/calc/ascii.html.

[78] LESSIG, *supra* note 65, at 36.

[79] If a key is (n) bits long, the number of possibilities is 2^n. For example, here, n=2, so there are $2^2 = 4$ possibilities ('00', '01', '10', and '11').

key; so even though a 2-bit key only yields four possibilities, a 56-bit key yields 2^{56}, or roughly 72 quadrillion possible combinations. Assuming that a modern computer could try one billion possible keys every second, guessing the key could still require more than 2 billion years.[80] For this reason, encryption systems with keys of 56 bits or longer are referred to as strong encryption.

Though it may seem like strong encryption would provide sufficient security, the preceding example assumes finding the key by brute force guessing. Using advanced mathematical and other techniques, like large-number factoring and parallel processing, can significantly speed up this process. In fact, the former government standard encryption algorithm, called the Data Encryption Standard (or DES), used a 56-bit key, and was eventually broken in less than 23 hours by the Electronic Frontier Foundation and Distributed.net in 1999.[81]

Further, encryption algorithms are subject to threats beyond just advancements in decryption techniques. An empirically-proven rule of thumb in the computing world states that computing power doubles every 18 months.[82] Extrapolating that trend, in 15 years computers will be 1,000 times more powerful than they are today. New decryption techniques coupled with ever-increasing computing power continued to threaten the security of existing encryption algorithms. In November 2001, the National Institute of Standards and Technology (NIST) replaced the existing DES with the new and improved Advanced Encryption Standard (AES) for encrypting classified government information.[83]

[80] For mathematical convenience, we are assuming (1) a computer has a 1 GHz processor (the processor runs at 1 billion clock-cycles per second); and (2) trying a possible key only requires a single clock cycle.

[81] *See* Wikipedia, EFF DES Cracker, http://en.wikipedia.org/wiki/EFF_DES_cracker (last visited Feb. 4, 2007); *but see*, Siewert, *supra* note 68 (DES was broken in *less than three hours* by DES Cracker). Ironically, three years earlier, William P. Crowell, Deputy Director of the National Security Agency stated: "If all the personal computers in the world . . . were put to work on a single [strong]-encrypted message, it would still take an estimated 12 million times the age of the universe, on average, to break a single message." *Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 695 before the Subcomm. on Courts, the Internet, and Intellectual Property of the H. Comm. on the Judiciary*, 105th Cong. 45 (1997).

[82] This rule is an adaptation of "Moore's Law," which comes from an article by Gordon H. Moore, an electronic engineer and co-founder of Intel Corporation. In the article, he stated that "The complexity for minimum component costs has increased at a rate of roughly a factor of two per year. . .," 38 ELECTRONICS 115, Apr. 19, 1965. Though Moore's law specifically relates to the number of transistors on an integrated circuit, the same concept has been empirically proven for other areas of technology. *See, e.g.*, Ray Kurzweil, *Human 2.0: The New Version is Coming Sooner Than You Think*, NEW SCIENTIST, Sept. 24, 2005; Ray Kurzweil, *The Law of Accelerating Returns*, Mar. 7, 2001, http://www.kurzweilai.net/meme/frame.html?main=/articles/art0134.html.

[83] NIST, *Announcing the Advanced Encryption Standard (AES)*, FIPS-197, Nov. 26, 2001.

The AES algorithm is based on a cipher known as Rijndael and supports key lengths of up to 256 bits. [84] AES is stronger, and less time- and memory-intensive to process than most of today's other strong encryption algorithms.[85] But how long will it remain secure? The goal of AES was to provide "agencies with a new encryption method designed to be secure for at least 20-30 years."[86] Only one year after its adoption as a standard, cryptographers had already begun to point out flaws in its strength.[87] These claims may be simply Internet machismo, as no published cracks exist yet for AES. Moreover, AES is still the standard for classified information.

Many other ciphers exist, but they are all essentially an algorithm with a key. The world of digital cryptography is a cat and mouse game; stronger ciphers are cracked by faster computers and more clever math, which lead to stronger ciphers. In the end, however, the fundamental flaw with all these encryption methods is that their strength is still based on the number of guesses required to crack the code.

C. Encryption's Death and Rebirth

> "Consequently, the development of a fully operational quantum computer would imperil our personal privacy, destroy electronic commerce and demolish the concept of national security. A quantum computer would jeopardise the stability of the world. Whichever country gets there first will have the ability to monitor the communications of its citizens, read the minds of its commercial rivals and eavesdrop on the plans of its enemies."[88]

With infinite computing power, any of these encryption methods could be cracked in an infinitely small amount of time.[89] Still, modern cryptography primarily relies on the limitations of computing power for

[84] *Id.*

[85] For a thorough description of the Rijndael algorithm, *see* Wikipedia, Advanced Encryption Standard, http://en.wikipedia.org/wiki/Advanced_Encryption_Standard (last visited Feb. 4, 2007).

[86] Office of Management and Budget, OMB Guidance to Federal Agencies on Data Availability and Encryption, http://csrc.nist.gov/policies/ombencryption-guidance.pdf (last visited Feb. 4, 2007).

[87] Dana Mackenzie, *A Game of Chance*, NEW SCIENTIST, June 7, 2003, at 36-39; Charles Seife, *Crucial Cipher Flawed, Cryptographers Claim*, 297 SCIENCE 2193 (Sept. 27, 2002).

[88] *See* Singh, *supra* note 64, at 331.

[89] Using the same conventions of computing power as above (*supra* note 79) a cipher with a key length of 128 bits would yield 340 trillion trillion trillion combinations (34 followed by 37 zeroes); and trying all the keys would require up to 700 billion times the age of the universe. However, if computers were ten trillion trillion (10^{25}) times faster, trying all the keys would only take about 9 hours.

its strength. "As information becomes the world's most valuable commodity, the economic, political and military fate of nations will depend on the strength of ciphers."[90] Thus, as computers get more powerful, the world falls increasingly into jeopardy. The rise of quantum computing, a new form of computing based on the laws of quantum physics, heralds an age when effectively infinite computing power will be available for cracking the world's largest codes.

Probably the most discussed difference between classical and quantum physics results from what is called the "Heisenberg Uncertainty Principle."[91] Classical physics assumes that a particle's state (its position and momentum) is known and observable. In quantum physics, however, the act of observing the particle affects its path. Thus, the more certain you are of the particle's position, the more uncertain you become about its momentum, and vice versa. A strange implication of this is that when the particle is not being observed, quantum physics says that particle is actually in multiple states simultaneously.[92] This may seem strange, or even like a matter of semantics, but there is a large practical difference. Without this difference, physics would be unable to explain many everyday effects ranging from nuclear power to lasers.[93]

Quantum computers rely on this quantum effect. A classical computer bit is either '1' or '0', like a coin which is either heads or tails. However, when no one is looking, a quantum computer bit (called a qubit) is both '1' and '0' at the same time, like a spinning coin which is effectively both heads and tails until someone stops the spin. If one qubit can be both 0 and 1 at once, seven qubits could be considered to simultaneously represent all the numbers from zero to 127.[94] Recall that the strength of classical encryption methods relies on the impracticality of trying a very large number of possible keys to decipher a message. Unlike a classical computer, which must try each key one-at-a-time to see if it works, a quantum computer could essentially try all possible

[90] *See* Singh, *supra* note 64, at 331.

[91] J. A. WHEELER & H. ZUREK, QUANTUM THEORY AND MEASUREMENT 62-84 (1983), at (*translating* W. Heisenberg, *Über den Anschaulichen Inhalt der Quantentheoretischen Kinematik und Mechanik*, 43 ZEITSCHRIFT FÜR PHYSIK 172 (1927)).

[92] A famous illustration of this is "Schrödinger's Cat." Imagine a cat in a ventilated, but opaque box. When the door to the box is closed, you cannot see the cat. You place a fragile vial of cyanide on the floor of the box. If the cat steps on the vial and releases the cyanide, it will immediately die. Is the cat alive or dead? In classical physics, the cat is either alive or dead. Quantum physics would say that when no one is looking, the cat is both alive and dead (or more accurately, the cat is in some superposition of the alive and dead states). When the box is opened, the cat immediately chooses either the alive or the dead state. *See id.* at 152-67 (translating the original E. Schroedinger, 23 NATURWISS. 807 (1935)).

[93] *See* Singh, *supra* note 64, at 325.

[94] Seven binary digits, can represent the decimal numbers from '0' (binary '0000000') to '127' (binary '1111111').

keys at the same time. In this way, quantum computers could be used to crack even the longest key-length ciphers in seconds, rendering classical encryption methods worthless.

Fortunately, however, that is not the end of the story for encryption. First, quantum computing is a nascent field, and the first quantum computers only exist in laboratory settings. Second, the properties of quantum physics also form the basis for a new fundamentally unbreakable class of cipher, known as quantum encryption. Quantum encryption utilizes the quantum properties of individual photons of light. The resulting transmission method is completely secure (the encryption is fundamentally unbreakable) for two reasons. First, because of the Uncertainty Principle, any attempt to eavesdrop will affect the contents of the message. By checking a relatively small sampling of transmitted data, the sender and receiver can detect surveillance attempts. Second, quantum properties of the photons allow the sender and receiver to overtly communicate one-time keys for each message without ever disclosing the values sent. For a more thorough description of how this works, see Appendix A.

For the vast majority of people, who cannot contemplate sending or measuring a single photon, quantum cryptography seems like something out of Star Trek. However, the first cryptographic message was sent using this scheme over fifteen years ago.[95] In the years since, the technology has significantly improved. At an information security conference in Geneva in April 2005, companies began releasing turn-key quantum encryption systems for use with existing Ethernet networks.[96] The products are fast enough to perform quantum encryption and eavesdropping detection for broadband time-critical applications like VoIP calls.[97] In addition to quantum cryptography for wired networks, there are high-speed wireless optical networks running quantum cryptography over distances of ten kilometers.[98]

For now, the average computer user does not have the capability or desire to hack into communications using even strong encryption. In fact, messages in transit are rarely intercepted.[99] However, law enforce-

[95] *See* Singh, *supra* note 64, at 347-48 (Charles Bennett and his graduate student, John Smolin, sent the first message from a computer named Alice to one named Bob in 1989).

[96] R. Colin Johnson, *Quantum Encryption Enters Product Phase*, ELEC. ENG'G TIMES, May 2, 2005, at 44.

[97] *Id.*

[98] Chappell Brown, *Wireless Quantum-Crypto Network is Live*, ELEC. ENG'G TIMES, June 13, 2005, at 58.

[99] Alison Diana, *Benchmarking Encryption Technology*, E-COMMERCE TIMES, Aug. 12, 2003, *available at* http://www.ecommercetimes.com/story/31311.html ("[Ray Wagner, research director for information security strategies at Gartner, said,] The likelihood of people attacking encryption in data transfer is relatively low. Most organizations could probably deploy 40-bit encryption and never have an attack against those types of data transfers. That

ment and others with a large interest in electronic surveillance will use whatever technology is available to get the job done. For example, though quantum computers are still in the experimental phase, when they do arrive, they will render strong encryption schemes impotent. On the other hand, today, users can employ strong encryption, which is effectively unbreakable, and quantum encryption, which is fundamentally unbreakable (even by a quantum computer). This provides a government policy incentive to limit the spread and effect of encryption, but, that said, similar policy directions have failed in the past.

D. Overview of United States' Encryption Policy

> "[A poll taken shortly after the September 11th attacks] asked: 'Would you favor reducing encryption of communications to make it easier for the FBI and CIA to monitor the activities of suspected terrorists—even if it might infringe on people's privacy and affect business practices?' Fifty-four percent of those polled answered 'yes,' and 72 percent said anti-encryption laws would be . . . helpful in thwarting similar terrorist attacks."[100]

As with surveillance regulation, encryption regulation must carefully balance individual privacy against national security. These concerns, as well as concerns from the U.S. encryption market, have driven the history of encryption legislation.[101] On the one hand, by using encryption, Internet users can freely engage in private communications with people around the globe. On the other hand, encryption technology impedes law enforcement's ability to intercept communications by criminals.[102] For example, the "widespread availability of strong encryption technology threatens to undermine the effectiveness of the money laundering controls currently in place."[103]

said, 40-bit encryption is not hard to break").

[100] Declan McCullagh, *Senator Backs Off Backdoors*, WIRED NEWS, *at* http://www.wired.com/news/conflict/0,2100,47635,00.html.

[101] David B. Walker, *Privacy in the Digital Age: Encryption Policy-A Call for Congressional Action*, 1999 STAN. TECH. L. REV. 3, 22-31 (1999).

[102] Jeffrey Yeates, *CALEA and the RIPA: The U.S. and the U.K. Responses to Wiretapping in an Increasingly Wireless World*, 12 ALB. L.J. SCI. & TECH. 125, 136-137 ("Modern communication systems are no longer wires connected to a switch, but are . . . an era of intelligent networks, . . . a digital environment that allows sophisticated encryption. . . . The rapid introduction of these technological innovations has injected difficulty into law enforcement's task of intercepting communications. . . . As noted earlier, the FBI disclosed to Congress at the CALEA hearings more than 180 instances of when it had been unable to intercept a communication because of technological impediments").

[103] Andres Rueda, *The Implications of Strong Encryption Technology on Money Laundering*, 12 ALB. L.J. SCI. & TECH. 1, 4 ("Strong encryption threatens current money laundering from two directions. Money laundering is typically perpetrated by exploiting the financial sys-

Currently, however, encryption use is not widespread. While many people use secure servers for financial transactions and password-protected files for secret information, few people encrypt email messages or VoIP phone calls. A likely reason is that there is currently no good push-button encryption program on the market. Encrypting email often requires special software, key management, or even the creation of scripted algorithms. Nonetheless, encryption technology is rapidly changing. If a push-button encryption solution becomes available, it may drive ubiquitous encryption usage.

Lawrence Lessig speaks of four different modalities of regulation: architecture (or "code"), market, legislation, and societal norms.[104] The government has attempted at least the first three in regards to encryption regulation. The first type of regulation involved the architecture, or "code" of encryption. The Clinton administration proposed a number of initiatives, beginning with "Clipper Chip" in 1993, and ending with "Clipper 3.1.1" in 1996.[105] The intent of the Clipper Chip proposals was twofold: The chip would be used in encryption systems to provide the government with a back door for access to encrypted files; and a Trusted Third Party (TTP) would be established to hold, in effect, a spare set of keys for each person using encryption to be used by the government if necessary to gain access to encrypted files (called key escrow).[106] The proposals all received vehement opposition from the software industry and various privacy-advocating organizations.[107] In response, Clinton pressured other countries to support the key escrow initiatives. This tactic failed. The Organization for Economic Cooperation and Development (OECD), the European Union, and the Wassenaar Arrangement Group (consisting of thirty-three industrialized nations) all supported other methods like industry- and market-based regulation; and by 1998, key escrow was dead.[108]

The second type of government-imposed regulation involved limits on the export market. Because of the importance of encryption to the military, the international proliferation of strong encryption was seen as a

tem's information technology network to obscure through multiple transactions the origin of dirty funds. Accordingly, strong encryption can be used to prevent the recovery by law enforcement of the evidence that could be used to convict money launderers").

[104] Lessig, *supra* note 65, at 87.

[105] *Id.* at 300.

[106] *Id.* at 300-01.

[107] *See, e.g.*, Rutrell Yasin, *Senators Pledge to Push Encryption Reform*, INTERNETWEEK, June 18, 1998; *EPIC's Challenge to the Secrecy of the Clipper Initiative*, *at* http://www.epic.org/crypto/Clipper/challenge.html; Shari Steele & Daniel J. Weitzner, *Chipping Away at Privacy*, http://www.cdt.org/crypto/admin/clipper.summary.txt (last visited Feb. 4, 2007).

[108] Tricia E. Black, *Taking Account of the World as It Will Be: The Shifting Course of U.S. Encryption Policy*, 53 FED. COMM. L.J. 289, 302 (2001).

threat to national security. The government thus decided that, while encryption sales should not be limited within the United States, its export should be. Prior to 1996, its export was restricted as a dual-use munition[109] (a technology with both military and commercial uses) under the Export Administration Regulations (EAR)[110] and the International Traffic in Arms Regulations (ITAR),[111] both of which administer the Arms Export Control Act (AECA).[112] However, by 1996, it had become clear that the world already had strong encryption, and export restrictions were only hurting U.S. encryption companies.[113] Thus, from 1996 to 2000, President Clinton eliminated the commercial encryption export restrictions to the European Union and eight other countries in an attempt to better balance security and U.S. economic needs.[114] Since that time, the courts have volleyed the question of Congress's Constitutional authority to regulate encryption and its export,[115] but little has changed since the end of the Clinton administration.

The final type of government-imposed regulation involves legislation. One of the most notable recent encryption-based attempts at legislation is the Security and Freedom Through Encryption (SAFE) Act, proposed in 1999.[116] This Act would officially rescind many previous regulatory attempts by removing export regulations, key length limits, and key escrow requirements.[117] Interestingly, no significant actions have been taken on this bill since it was placed on the Union Calendar in July 1999.[118] Few other bills focusing primarily on encryption have been

[109] *Id.* at 298-99.

[110] Export Administration Regulations (EAR), 15 C.F.R. pts. 730-74.

[111] International Traffic in Arms Regulations (ITAR), 22 C.F.R. pts. 120-30.

[112] Arms Export Control Act (AECA), 22 U.S.C. §§ 2751-2796c (2000).

[113] Rueda, *supra* note 103, at 4-5; s*ee also*, Junger v. Daley, 209 F.3d 481 (6th Cir. 2000); Karn v. United States Dep't of State, 925 F. Supp. 1 (D.D.C. 1996), *remanded in*, 107 F.3d 923 (D.C. Cir 1997).

[114] Black, *supra* note 108, at 299-300.

[115] *Compare* United States v. Odutayo, 406 F.3d 386, 391-392 (5th Cir. 2005) ("The interest in the regulation of the exportation of weapons, ammunition, and encryption technology, similar to the interest in the flow of currency, represents the fundamental power—indeed, responsibility—of every sovereign nation to maintain its national security."), *with* Universal City Studios v. Reimerdes, 111 F.Supp.2d 294, 304-305 (S.D.N.Y. 2000) ("In an era in which the transmission of computer viruses—which . . . are simply computer code and thus to some degree expressive—can disable systems upon which the nation depends and in which other computer code also is capable of inflicting other harm, society must be able to regulate the use and dissemination of code in appropriate circumstances. The Constitution, after all, is a framework for building a just and democratic society. It is not a suicide pact").

[116] Security and Freedom Through Encryption (SAFE) Act, H.R. 850, 106th Cong. (1999). This bill, proposed by Representatives Bob Goodlatte and Zoe Lofgren, is similar to H.R. 695 (105th Cong.) and H.R. 3011 (104th Cong.).

[117] *See SAFE HR 850*, *at* http://www.cdt.org/crypto/legis_106/SAFE/.

[118] *See* Library of Congress, Major Actions for H.R. 850, *at* http://thomas.loc.gov/cgi-bin/bdquery/z?d106:HR00850:@@@R.

proposed, especially in recent years.

As encryption regulation continues to weaken, public access to effectively unbreakable encryption continues to rise. Further, while weak surveillance regulation hurts privacy,[119] weak encryption policy creates the potential for stronger privacy. Thus, as long as the public is able to take advantage of the current access to encryption technology, the opportunity exists to counteract the erosion of privacy rights from increased surveillance. The privacy-restorative potential of encryption in the face of surveillance is the focus of Section IV.

IV. STRONG ENCRYPTION CAN RESTORE THE PRIVACY-SECURITY BALANCE

> "[C]riminals are increasingly using encryption technologies to conceal their activities and thwart law enforcement efforts to collect critical evidence needed to solve and prosecute serious and often violent criminal activities. The potential use of unbreakable encryption products by a vast array of criminals and terrorists, to conceal their criminal communications and information, poses an extremely serious threat to public safety and national security."[120]

In 2004, graduate students at the University of Colorado examined various options for making VoIP phone calls.[121] The so-called "softphones" used to make VoIP calls come in a variety of forms, including using either open- or closed-source code, centralized or decentralized networks, and free or paid services. After attempting methods for applying end-to-end encryption to secure those calls, the graduate students concluded that:

> [T]here are several readily available tools and methods with which to create a strongly encrypted Internet voice call. Though limited in number now, more of these tools are being created with each passing season. Many of these methods are so basic that any attempt to ban or alter them would profoundly affect the Internet as a whole. At this point in time and in the future, *we believe that two end users using public domain tools and minimum setup can effectively create an*

[119] *See supra* Part II.

[120] Jessica R. Herrera, *International Aspects of Cybercrime*, *in* CYBERCRIME 172 (Ralph D. Clifford ed. 2001).

[121] Matthew Bates & Thiha Min, *Problems with Wiretapping of VoIP Services* (Univ. of Colorado Policy Lab, Working Paper, Summer 2004), http://www.colorado.edu/policylab/Papers/Secure_Voip_writeup%20v3_2%20_2_.pdf (emphasis in original).

> *Internet call that cannot be wiretapped.*[122]

This study has clearly devastating implications for the efficacy of electronic surveillance as applied to the Internet. Consider this hypothetical: The NSA suspects a professor at a university is laundering funds for terrorist organizations, and they want to listen in on his VoIP phone calls. The NSA would have two hurdles to overcome.

First, the NSA must have some authorization to perform electronic surveillance. Under the Federal Wiretap Act or the original language of FISA, the NSA would be required to get a court order to avoid violations of procedural privacy (essentially a warrant for their electronic "search"). Arguably, under FISA as amended by the Patriot Act, there may be a blanket executive order to engage in this activity to combat terrorism. Either way, the trend of weakening surveillance regulation suggests that this would be an easy hurdle to clear.

Armed with authority, the NSA would have to then overcome the second hurdle: performing the actual surveillance to obtain information. After compliance with the CALEA Order, the university would have back doors built into its network. The NSA would patch surveillance equipment into the university's network and begin to monitor VoIP traffic to and from the professor to hopefully gain evidence of his money laundering. Without encryption, this would also be a simple hurdle, rendering the professor's privacy protections impotent. However, using free, publicly-available software, and minimal effort, the professor could encrypt all his VoIP phone calls. With today's strong encryption, the content of these calls would be essentially indecipherable,[123] and therefore useless to the NSA.

Thus, encryption technology has the ability to restore many of the privacy-erosive effects of lax surveillance regulation. Unfortunately, most people tend not to use adequate encryption to protect their Internet traffic. Fortunately, however, the growth of the Internet and the development of push-key encryption may cause that tendency to change.

A. The Rise of Data Threats Will Cause People to Use More Encryption

> "What could quantum physics and Paris Hilton possibly have in common? The Hilton hotel chain heiress and Hollywood starlet got a bonus 15 minutes of fame a few weeks ago after hackers burrowed their way into her mobile phone, stealing her celebrity contact information and distributing it across the Internet. Her experience raised

[122] *Id.* (emphasis in original).
[123] *See supra* Section III.

> an issue few had contemplated before – That evil techies bent on doing bad things can unlock the contents of a cellphone, Blackberry or wireless PDA just like any other computer system or network."[124]

It is hard to say how many people are using encryption today. Whether or not they are, however, it seems likely that encryption use will rise dramatically in coming years. There are three reasons for this prediction. First, many companies in select industries have adopted encryption standards to avoid liability under various pieces of legislation.[125] In September 2005, for example, the three largest credit reporting agencies pledged to adopt a standard encryption system to protect credit information.[126] Second, though implementing encryption in a large corporation can raise storage and data processing costs, encryption hardware and software is relatively inexpensive;[127] with many corporations employing free algorithms from the Internet,[128] and some purchasing even the newest quantum devices for under $100,000.[129] Ultimately, however, the third reason—fear—will likely be the biggest driving force for adopting encryption.

The ubiquity of the Internet and digital communication means that more digital data is being transmitted around the globe than ever before. Much of this data supports a new economy, including efficient international property transfers and electronic commerce. With that increase in data has come an increase in the danger of identity theft. Public fear of identity theft has, in turn, become a "killer app" for the adoption of encryption.[130]

[124] M. Corey Goldman, *A Quantum Leap for Computer Security; Powerful Chips Perversely Make Hacking Easier. Here's a System that, for Now, Is Said to Make It Impossible*, TORONTO STAR, Mar. 7, 2005, Business, at 1.

[125] Jay Lyman, *FTC: Identity Theft Worse than Estimated*, E-COMMERCE TIMES, Sept. 4, 2003, *available at* http://www.ecommercetimes.com/story/31498.html.

[126] Reuters, *Credit Bureaus to Adopt Data Protection Standard*, CNET, Sept. 22, 2005 ("The coordinated effort by the three traditional rivals is the latest proof of the serious threat posed by identity thieves and Internet-enabled crooks. . . ."), *available at* http://news.com.com/2100-1029_3-5877870.html.

[127] Alison Diana, *Benchmarking Encryption Technology*, E-COMMERCE TIMES, Aug. 12, 2003 ("Indeed, although the cost of encryption technology . . . is negligible, implementing it can lead to higher storage and processing costs."), *available at* http://www.ecommercetimes.com/story/31311.html; *but see* Bruce Schneier, *Information Security: How Liable Should Vendors Be?*, COMPUTERWORLD, Oct. 28, 2004.

[128] *See, e.g.*, http://www.cypherix.com/cryptainerle/ (Cryptainer LE from Cypherix Products); http://www.freebyte.com/security/#freeencryption (contains a list of free file encryption programs).

[129] Jack Mason, *Quantum Cryptography Companies Tap into Nanoscale's Quirky Core*, SMALL TIMES, Feb. 19, 2004, *available at* http://www.smalltimes.com/document_display.cfm?section_id=47&document_id=7448.

[130] The phrase "killer app" generally refers to an application which will drive the market for a certain platform technology. A classic example is the "Super Mario Bros." game for the Nintendo video game system.

The threat of identity theft moved even further to the forefront of public consciousness in the wake of several headline-grabbing, high-profile data breaches. In February 2005, ChoicePoint, Inc., a company which ironically claims to be the "leading provider of identification and credential verification services,"[131] announced that a security breach left the personal information of 145,000 Americans vulnerable to identity thieves.[132] Then, in May 2005, Bank of America announced that over 60,000 of their customers were data breach victims, those customers joining approximately 676,000 victims of a New Jersey data-theft ring.[133] Later that month, data tapes which archived personal information for 3.9 million Citigroup customers literally fell off the back of a UPS truck,[134] and a laptop was stolen from Omega World Travel, which contained the names and credit card numbers of approximately 80,000 employees of the U.S. Department of Justice.[135] Only a couple of weeks later, a number of credit card companies began accusing CardSystems of negligently allowing a breach to compromise 40 million credit card accounts.[136] The stories continued to pile up, and within one year of the ChoicePoint incident, data breaches had claimed 55 million victims.[137]

Individuals were not the only victims of the data breaches. The breached companies incurred enormous losses, both in terms of money and goodwill. Following their respective incidents, ChoicePoint paid $15 million in fines to the FTC,[138] over 50,000 customers closed their Citigroup accounts,[139] and "CardSystems has nearly been forced out of existence as business partners have fled."[140]

To avoid these significant losses, businesses have begun to look to encryption as an essential information security component. There are

[131] *See* ChoicePoint, http://www.choicepoint.com/ (last visited Feb. 4, 2007).

[132] Rachel Konrad, *Burned by ChoicePoint Breach, Potential ID Theft Victims Face a Lifetime of Vigilance*, THE ASSOCIATED PRESS (Feb. 24, 2005), *available at* http://www.securityfocus.com/news/10552.

[133] Todd R. Weiss, *Bank of America Notifying 60,000 Customers About Stolen Data*, COMPUTERWORLD (May 24, 2005), *available at* http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,101992,00.html.

[134] *Info on 3.9M Citigroup Customers Lost*, CNN MONEY (June 9, 2005), *available at* http://money.cnn.com/2005/06/06/news/fortune500/security_citigroup/index.htm.

[135] Weiss, *supra* note 133.

[136] Jason Krause, *Law Firms Face Cyberthreats*, *in Flying Under the Radar: These Little-Noticed Legal Developments Could Be Making News this Year*, 92 A.B.A.J. 34 (2006).

[137] *See* Privacy Clearinghouse Report, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Feb. 4, 2007). The 55 million victims include targets of data crimes which are not the result of mismanagement, like phishing and pharming on people's home computers (Last visited Feb 3, 2006).

[138] Bob Sullivan, *ChoicePoint to Pay $15 Million over Data Breach*, MSNBC (Jan. 26, 2006), http://www.msnbc.msn.com/id/11030692.

[139] *Info on 3.9M Citigroup Customers Lost*, *supra* note 134.

[140] Krause, *supra* note 136.

two main reasons to choose encryption. First, the adoption of encryption is a clear sign to the public that something is being done to protect their data. For example, after its data breach, Citigroup released a press statement stating that "[b]eginning in July, this data will be sent electronically in encrypted form."[141] Second, a number of information security-related statutes mention encryption as a necessary component of enterprise data security. One example at the Federal level is the Consumer Data Security and Notification Act of 2005, part of which amends the Fair Credit Reporting Act and the Gramm-Leach Bliley Act to give more explicit guidance for the use of encryption.[142] At the state level, encryption can be even more important for companies. Under California's breach notification law, for example, companies which encrypt their data are exempt from disclosing breaches to their customers in many cases.[143]

As the demand for encryption increases, so will the incentive for developers to create effective, inexpensive, push-key encryption solutions. Hopefully, consumers will begin to adopt and use those new solutions to protect their communications from unauthorized surveillance. In that way, the encryption will be able to serve its privacy-restorative function. With undecipherable encryption, it may seem that all hope is lost for law enforcement—that ubiquitous encryption will so tilt the balance towards privacy that National security will suffer. This is not the case. Many options still exist for law enforcement even in a world of ubiquitous encryption.

B. Even with Ubiquitous Encryption, Law Enforcement Has Options

> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. . . . You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is differ-

[141] Kevin Kessinger, Executive Vice President of Citigroup's Global Consumer Group and President of Consumer Finance North America, quoted in a statement by CitiGroup Inc., June 02, 2005, *available at* http://www.citigroup.com/citigroup/press/2005/050602e.htm.

[142] *See* Consumer Data Security and Notification Act of 2005, H.R. 3140, 109th Cong. (2005).

[143] *See* CAL. CIV. CODE § 1798.82.

ent."[144]

There are three likely outcomes to the privacy issues generated from the trend towards lax surveillance regulation. The first would be the most dire and hopefully least likely: The trend will persist, allowing law enforcement increased access to private communications, and the public will fail to widely adopt encryption. This outcome would be the most privacy erosive, and would allow law enforcement to surveil the public with extreme ease. The second outcome would be a change in the direction of the trend. A number of lawsuits have already been filed against the FCC, challenging its authority and the constitutionality of the Order.[145] If these suits succeed, privacy will have won a battle, but the war will continue in the jungles of ever-present privacy-invasive legislation. Another terrorist attack, or other invasion of national security, may prompt even more invasive legislation. Finally, the third outcome would be perhaps the most interesting, and arguably the most sustainable; that the CALEA Order will persist, but the public will move towards ubiquitous strong-encrypted communications.

Either the second or third outcome would debilitate a very important tool of law enforcement. To combat that result, the law enforcement community would have to find another way to get the information they want from criminals. One solution is to once again try to regulate encryption. The government may provide benevolent social justifications for regulating encryption beyond just better surveillance of criminals. It may claim the importance of preventing the potentially false sense of security people feel from encrypted data,[146] the facilitation of faster access to important information (like medical records),[147] or even the preservation of the public domain which should not be subjected to potential obfuscation through encryption.[148] However, the past has shown that regulations on encryption are not a good idea. Encryption allows persecuted

[144] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, Feb. 8, 1996, http://homes.eff.org/~barlow/Declaration-Final.html.

[145] Caron Carlson, *ACLU Joins Fight Against Internet Surveillance*, EWEEK.COM, Dec. 1, 2005, *available at* http://www.eweek.com/article2/0,1895,1895253,00.asp.

[146] Paul F. Roberts, *MCI Data Theft Intensifies Encryption Debate*, EWEEK.COM, May 31, 2005, *available at* http://www.eweek.com/article2/0,1759,1821333,00.asp (A California statute, for example, allows companies to forgo notifying customers of data security breaches if they are using encryption.).

[147] Paul Roberts, *Electronic Medical Record Keeping Places Demands on IT Execs at Hospitals*, INFOWORLD, Sept. 7, 2004, *available at* http://www.infoworld.com/article/04/09/07/HNmedicalrecord_1.html?s=feature (discusses balance between access and privacy of medical records); *see also*, R. M. Califf and L. H. Muhlbaier, *Health Insurance Portability and Accountability Act (HIPAA): Must There Be a Trade-Off Between Privacy and Quality of Health Care, or Can We Advance Both?*, 108 CIRCULATION 915-918 (2003).

[148] *See, e.g.*, Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 156 (1975).

populations more freedom through anonymous and pseudonymous communication;[149] it facilitates the establishment of private data domains which may be controlled by trespass law or the Fourth Amendment; and it encourages the creation of copyrighted data by protecting authors from unauthorized copying and distribution.[150] Even more importantly, government attempts at regulating encryption in the past have been disasters.[151]

Even though Congress is unlikely to attempt future wide-scale regulations on encryption for the above reasons, there are two other potential possibilities. One possibility would be to help protect security and law enforcement by legislating the effects of encryption. For example, the White House recently announced legislation to give "$80 million over four years for a research center to help law enforcement agencies learn how to crack encryption. . .[, to] create a legal framework that would allow the police to have 'back doors' under certain conditions. . .[, and to] ensure that sensitive investigative techniques . . . remain useful and secret by protecting them from forced disclosure in criminal and civil litigation."[152] The second possibility would be to promote ubiquitous encryption use. This would greatly enhance the potential for privacy, while simultaneously forcing law enforcement to find new ways to obtain information without the aid of domestic electronic surveillance.

Importantly, even if strong encryption usage forces law enforcement to find other methods of surveillance, many options still exist. These options arise from the fact that the types of strong encryption discussed thus far assume the information is in transit. A communication, however, transpires in five stages: (1) the sending party enters the information into a device; (2) the sending party's device stores the information either in permanent or temporary storage on a device; (3) the device takes the information from storage and sends it to the receiving party's device; (4) the receiving party's device stores the information in permanent or temporary storage; and (5) the receiving party views or listens to the information. The information is only in transit during stage (3). New techniques can still provide surveillance options during the other stages of

[149] Human Rights Watch, *Crypto Controls Threaten Human Rights*, HUMAN RIGHTS NEWS, Sept. 18, 1998, *available at* http://hrw.org/english/docs/1998/09/18/global1297.htm (HRW is a non-profit organization that investigates and reports violations of human rights in over 70 countries worldwide. In this article, Jagdish Parikh, online research associate at Human Rights Watch states that "Encryption is more than a shield for human rights activists, . . . [c]oded language is still language, and it must be protected as a basic human right to free expression.").

[150] MGM Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2795 (2005) ("Other technology can, through encryption, potentially restrict users' ability to make a digital copy").

[151] Part III discussed some of the issues the government faced with regulations on the export and architecture of encryption (like the Clipper Chip and Key Escrow proposals).

[152] MARK GROSSMAN, TECHNOLOGY LAW 137-38 (2004).

the communication when the information is at the end points. For example, law enforcement could use a key-logger to capture keystrokes as the sending party types information into the device in stage (1).[153] Other end-point surveillance possibilities include using spyware and Trojan programs which invade the end user's device and give back-door access to other party's, and even using detectors to listen to the high frequency radiation of computer monitors to remotely "see" what the user is seeing.[154]

Assuming the trend continues toward lax surveillance regulation, privacy protection will remain in the hands of the public. People will be forced to either preserve their own privacy through means including encryption, or subject their communications to potentially limitless government surveillance. If, as hoped, they choose the former, the government will still have surveillance options. The effects of ubiquitous encryption use, however, will be able to limit to privacy-erosive effects of those options and help restore the privacy-security balance.

CONCLUSION

> "[W]hile, of course, the law needs to keep pace with changing technology to ensure that government agencies have access to information to prevent crime and terrorism, the law also needs to keep pace with changing technology to protect privacy. . . ."[155]

Only a half-decade ago, communication technology looked vastly different from the technology of today. Most private communication occurred over wires, voice traffic and data traffic were technologically divergent entities, and government surveillance was severely restricted. Gathering private information about a person used to require trespassing onto property or myriad hours of surveillance, hoping to piece together shreds of data. Digital convergence and the Internet have set the stage for revolutions in data types, data quantities, and the media through which data travels. For the world of surveillance, this has created a flood of names, addresses, credit scores, and conversations on our public wires and airwaves.

As surveillance regulations continue to weaken, the ability of law enforcement to ignore the privacy rights of individuals continues to increase. However, effectively unbreakable encryption could limit the pri-

[153] *See*, *e.g.*, United States v. Scarfo, 263 F.3d 80 (3d Cir. 2001) (involved the use of key loggers by the FBI).

[154] *See*, *e.g.*, Wikipedia, Computer Surveillance, http://en.wikipedia.org/wiki/Computer_surveillance (last visited Feb. 4, 2007).

[155] *Oversight Hearing on Implementation of the USA Patriot Act*, *supra* note 29.

vacy-erosive effects of this surveillance, but only with its ubiquitous adoption by the public. The trend in surveillance regulations illustrates law enforcement's assumption that the world of encryption will remain non-user-friendly, allowing surveillance to remain a critical tool for security. Hopefully, this prediction will prove to be incorrect, and the public will choose to take control of their privacy rights.

With ubiquitous encryption usage, the pendulum will swing back towards a privacy-protective environment, and a new crossroad will emerge. Worldwide political dissidents and persecuted individuals will again be able to communicate with impunity, but so will money launderers, sex offenders, and terrorists. The government will have to choose to regulate encryption or support it. The former would mark an unfortunate reversion to past types of restrictions on encryption use, but the latter may herald a new world of privacy—one in which encryption is regaled as a privacy shield against erosive surveillance.

APPENDIX A. A BRIEF EXPLANATION OF QUANTUM CRYPTOGRAPHY

> "I think I can safely say that nobody understands quantum mechanics"[156]

To understand quantum encryption, it is helpful to think of light as individual photons, which move in a direction while vibrating. The direction of vibration is known as polarization.[157] Polarized filters, like those on many sunglasses, only allow photons with certain polarizations to pass through. Photons with a polarization perpendicular to the filter will be blocked, but certain other polarizations will be twisted to align with the filter and pass through.

Say that Alice has a computer from which she can send individual photons through one of two filter modes.[158] In mode one, photons either vibrate vertically ('|'), representing a '1', or horizontally ('-'), representing a '0'. In mode two, photons either vibrate diagonally-left ('\'), representing a '1', or diagonally-right ('/'), representing a '0'. Alice wants to send a message to Bob, who has a similar computer. There are five steps. In step 1, Alice sends random 1's and 0's, randomly switching between filter modes. Bob does not know which modes Alice will choose, so he randomly switches filter modes, as well. Sometimes he chooses the correct mode, and, as a result, measures the correct value ('1' or '0'). Other times, he chooses the incorrect mode, twists the polarization of the photon, and measures a value which may or may not be correct. In step 2, Alice calls Bob and they tell each other which modes they used (but not which values Alice sent). They know that they can only rely on the data Bob received when he picked the correct mode. In step 3, they discard all the values Alice sent when Bob picked the wrong mode (for example, Alice originally sent 1,000 photons and only 573 remain). Now they have created a random 573-bit key which only Alice and Bob know. Because of the fact that picking the wrong mode twists the polarization of the photon, it is nearly impossible to eavesdrop without affecting the data. Imagine that Eve had been listening on the line. She had randomly switched between filter modes, too, but every time she picked the wrong one, she unknowingly twisted the polarization of the photon being transmitted. In some of those cases, Bob and Alice would have the same

[156] Attributed to Richard Feynman, considered to be one of the greatest physicists of the 20th Century.

[157] In reality, light has the characteristics of both particles and waves, and has some very strange behaviors at the quantum level.

[158] This description is based on the work of Charles Bennett and Gilles Brassard, the inventors of quantum cryptography, as related in Singh, *supra* note 64, at 339-47.

mode, but different values.[159] Therefore, in step 4, Alice and Bob call each other again and verify some relatively small random subset of values from the key (say, 75 out of the 573 in the key). If any value does not match, the entire key is discarded, and Alice and Bob know they are being bugged. If all the values match, they can be almost certain that the line is secure. With a secure line, they continue with step 5, in which they use their key to encrypt and transmit one message. Afterwards, they throw away the key, and start over to create a new key for each new message.

[159] For example, for Alice's 439th photon, she sends a '1' by sending a photon with a diagonal-left polarization. Eve uses her '+'-shaped filter, which inadvertently and unknowingly twists the polarization, and may either measure a '1' or '0'. At the other end, Bob happens to pick the correct mode (his 'X'-shaped filter), which inadvertently and unknowingly re-twists the polarization, but to horizontal instead of vertical (representing a '0' instead of a '1'). The result is that after step two, they would see that Bob had picked the correct mode for measuring photon 439, and they would incorrectly assume that he had the correct value.