March 1998

Cryptography: "Key Recovery" Shaping Cyberspace (Pragmatism and Theory)

Kenneth P. Weinberg

Follow this and additional works at: https://digitalcommons.law.uga.edu/jipl

Part of the Intellectual Property Law Commons

Recommended Citation
Available at: https://digitalcommons.law.uga.edu/jipl/vol5/iss2/11

This Notes is brought to you for free and open access by Digital Commons @ Georgia Law. It has been accepted for inclusion in Journal of Intellectual Property Law by an authorized editor of Digital Commons @ Georgia Law. Please share how you have benefited from this access. For more information, please contact tstriepe@uga.edu.
CONTENTS

I. INTRODUCTION .......................... 669

II. SETTING THE VIRTUAL STAGE—AN INTRODUCTION TO TODAY’S INFORMATION-ORIENTED SOCIETY (CYBERSPACE & THE INTERNET) ......................... 670
   A. CYBERSPACE .................................. 670
   B. THE INTERNET AND THE GROWTH OF CYBERSPACE 671
   C. SUMMARY .................................... 673

III. THE ENCRYPTION DEBATE ....................... 673
   A. WHAT IS ENCRYPTION? ......................... 673
   B. WHY IS ENCRYPTION NECESSARY ON THE INTERNET? 675
      1. Effecting Individual and Business Finances On-line ........................ 675
      2. Effecting the Growth of Electronic Commerce ............................. 678
      3. Protecting Information in Order to Protect People 679
      4. Summary .................................... 680
   C. WHY WOULD THE GOVERNMENT WANT TO LIMIT ENCRYPTION TECHNOLOGY (POLICING CYBERSPACE)? 680
      1. The Internet and Interconnection ............................ 682
      2. The Problem with Cyber-evidence .............................. 683
      3. Summary .................................... 683

IV. THE PRAGMATIC DEBATE OVER THE PROPOSED SOLUTION— IS "KEY RECOVERY" REALLY THE KEY? ............... 683
   A. WHAT IS "KEY RECOVERY"? ...................... 684
   B. PRAGMATIC ARGUMENTS AGAINST "KEY RECOVERY" 685
      1. Imminent Doom of "Key Recovery" ........................... 685
      2. The Costs of Attempting to Build a "Key Recovery" Infrastructure .... 687
      3. Summary .................................... 688

667
V. A THEORETICAL ARGUMENT AGAINST "KEY RECOVERY"—THE ELIMINATION OF PHYSICAL BARRIERS AND THE INEFFICIENCY OF LEGAL CONSTRAINTS .............. 688
   A. HOW THE BARRIERS OF CYBERSPACE DIFFER FROM THE BARRIERS IN THE REAL WORLD (NATURE VS. CODE) .. 689
   1. Constraints in Real Space ....................... 689
   2. Constraints in Cyberspace ....................... 690
   3. An Important Difference ......................... 690
   B. KEY RECOVERY AND ITS EFFECT ON THE PHYSICAL LIMITATIONS OF CYBERSPACE ..................... 690
   1. Current Limitations in Real Space ............... 690
   2. Cyberspace Surveillance ......................... 691
   C. LEGAL LIMITS ARE NOT SUFFICIENT ............... 694
      1. Wire-Tapping Technology—Breaking Down Physical Barriers and Reformulating the Right to Privacy From a Property-Based Regime to an "Expectations" Regime .................. 694
      2. What is a Reasonable Expectation of Privacy: Infra-red and Electromagnetic Detection Devices—The Elimination of Physical Barriers Resulting in a Struggle to Define the Fourth Amendment .... 696

VI. CONCLUSION ........................................ 699
We are in the midst of a revolution. The Internet, often referred to as the information superhighway, is dramatically changing the informational structure of our society. Of course, heated debates often accompany drastic change, and our current technological evolution is no different.

One of the largest contemporary issues relating to the Internet stems from the use of encryption technology. On one hand, many people feel that this technology has become an indispensable part of the Internet. On the other hand, encryption sometimes thwarts law enforcement's attempts to police Cyberspace. As a result, the government has produced various proposals intended to balance these competing interests. The most recent proposal, referred to as "key recovery," has been the topic of much controversy.

The purpose of this Note is not only to summarize the encryption debate, but also to offer new insight into an issue that may very well shape the future of our society. For those readers who are not familiar with the encryption debate, this Note should provide the necessary framework to understand the issues and appreciate their importance. For those readers who have been following the debate, this Note will help organize the material and point out new arguments against "key recovery."

Section II of the Note briefly describes Cyberspace and the Internet. Section III sets the stage for the encryption debate by defining cryptography (the study of encryption), discussing the ways in which encryption is a necessary component of Cyberspace, and describing the government's reasons for wanting to limit the use of encryption. Section IV begins the analysis of the encryption debate by introducing the government's "key recovery" proposals, and providing a detailed discussion of various pragmatic arguments marshaled by opponents of "key recovery." Section V offers a more theoretical critique of "key recovery" by arguing that a "key recovery" system would result in the elimination of all physical limitations on the government's surveillance capabilities. A Fourth Amendment analysis of how courts have struggled with legal

1 The government has sought to resolve the encryption debate through legislation which would require the implementation of "key recovery" technology.
limitations when physical barriers are removed suggests that it would be extremely unwise to rely solely on legal limitations to protect the privacy of United States citizens. Finally, Section VI concludes this Note with a brief summary.

II. SETTING THE VIRTUAL STAGE—AN INTRODUCTION TO TODAY’S INFORMATION-ORIENTED SOCIETY (CYBERSPACE & THE INTERNET)

The terms “Cyberspace” and “the Internet” are commonplace in today’s society. Indeed, it sometimes seems as if everyone is talking about the “information superhighway” and various journeys into Cyberspace. Strangely, as the information age comes rushing upon us, few people can accurately define such terms.

The purpose of this Note is to help the reader understand the potentially tremendous impact that the current encryption debate may have on the future of our society. In order to understand these ramifications, the reader must have a clear understanding of the terms “Cyberspace” and “the Internet.” Therefore, this next section defines Cyberspace, discusses its revolutionary character, and describes how the unique structure of the Internet has contributed to the expansion of this new medium.

A. CYBERSPACE

The very word “Cyberspace” sounds like terminology from Star Trek or some other futuristic science fiction story. Indeed, the term was actually coined by science fiction writer William Gibson.2 One day Gibson wandered past some arcades and was struck by the intensity of the children who were playing the video games, noting that “[t]hese kids clearly believed in the space the games projected.”3 Gibson, who wrote Neuromancer on a manual typewriter, knew very little about computers.4 Nonetheless, he eventually concluded that everybody who used them with any frequency “develop[ed] a belief that there’s some actual space behind the

3 Next stop: Cyberspace, TIME, Mar. 9, 1998, at 172 (emphasis in original).
4 Id.
screen . . . that you can't see but you know is there."5 Gibson labeled this place "Cyberspace."

More technical definitions of Cyberspace describe it as "the conceptual space where words, human relationships, data, wealth, and power are manifested by people using computer technology."6 But what is "conceptual space," and how is it different from any other forum in which human relationships are manifest? The answer to this question rests upon an understanding of computer technology.

At the most basic level, the invention of computer technology resulted in the birth of electronic bits. "[A] bit has no color, size, or weight, and it can travel at the speed of light. It is the smallest atomic element in the DNA of information."7 These bits can be used in such a manner that very different forms of information can be expressed within the same medium.8 Bits can be utilized to integrate "text, graphics, sound and video into a single computing environment."9 This environment, commonly known as "Cyberspace," is revolutionary precisely because of this ability to communicate diverse expressions of information. Indeed, the advent of fiber-optic cables (which allow for bits to be transmitted even more quickly) makes it "conceivable that a single transmission medium could become the conduit for newspapers, electronic mail, local and network broadcasting, video rentals, cable television and a host of other information services."

B. THE INTERNET AND THE GROWTH OF CYBERSPACE

The ability to express various types of information within one medium becomes especially revolutionary if that medium is

---

5 Id.
8 Id. at 466-67 (noting that bits can be made to represent a variety of atom-based objects or analog forms of information such as speech, text music, photographs, and video).
9 Johns, supra note 6, at 1388.
available globally. By linking millions of computers and modem owners around the world, the Internet provides global access to Cyberspace and has become its most prominent part.

Perhaps the best way to understand the Internet is to study its origin. The Internet was created by the Department of Defense's Advanced Research Project Agency ("ARPA") in 1968. The goal of "ARPA's" creation was "to establish an open and accommodating global communications network of trusted hosts, including military installations, university researchers, and defense contractors." The Department of Defense wanted these hosts to be able to communicate after a nuclear war, so "ARPA" created a system which did not depend upon a centralized computer. Rather, any computer could route or re-route the information to its destination.

This unique structure has two important results. First, the fact that any computer can route information makes the Internet a two-way medium, allowing users to interact with other computers. This interaction grants Internet users unparalleled capabilities to retrieve information. For example "if a customer is looking to buy a car, he or she can do research on or even take a virtual test drive of the car, join a chat group, order the car, and arrange the financing from a bank—all from a home PC linked to the Internet."

Second, the fact that there is no centralized computer enables the Internet to grow in a manner which resembles an organism. Computers do not connect to a central location. Rather, they can connect with any computer which is linked to the Internet. As such, the Internet continues to grow at an exponential rate.

---

12 Goodman, supra note 7, at 482.
13 Id. at 482-483.
14 Hodkowski, supra note 11, at 222 (noting that "information is transmitted by being bundled into discrete ‘packets,’ each of which is routed from source to destination independently ... and recombined with other packets by the destination computer to reconstruct the entire transmission").
16 Johns, supra note 6, at 1388.
1983, only 562 computers were connected to the Internet. Now, we are "mov[ing] toward a billion connected [personal computers]."

C. SUMMARY

Hence, the invention of computer technology resulted in bits and the capacity to express diverse types of information within a single medium. This medium, commonly known as "Cyberspace," continues to grow at exponential rates due in large part to the Internet, which allows millions of computers to communicate in a two-way medium.

III. THE ENCRYPTION DEBATE

One of the most heated debates relating to Cyberspace and the Internet surrounds the use of encryption technology. This section sets the stage for the debate by defining cryptography, outlining the justifications for the use of encryption, and describing the government's interest in limiting the use of this technology.

A. WHAT IS ENCRYPTION?

Cryptography, the study of encryption, is an esoteric field of mathematics whereby individuals make and break codes through the use of mathematical algorithms.

An algorithm is a mathematical function which transforms information from one form to another.\(^\text{18}\) For example, the word "code" can be changed to "frgh" by the simple algorithm "?3?" which would result in a shift of each letter in the alphabet by three. The letter "c" becomes "f"; "o" becomes "r"; "d" becomes "g"; and "e" becomes "h".\(^\text{19}\)


\(^{18}\) Michael Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 U. PA. L. REV. 709, 714 (1995) ("An algorithm is a more formal name for a cipher.") (emphasis in original). See also WEBSTER'S NEW COLLEGIATE DICTIONARY 200 (1981) (defining a cipher as "a method of transforming a text in order to conceal its meaning.").

\(^{19}\) Of course, complex mathematical formulas can be used (instead of the simple letter shift above) to create a much more scrambled message.
A cryptosystem is a collection of different algorithms\(^{20}\) which enables an individual to "encrypt" a message by transforming its original form (called plaintext\(^{21}\)) into an unreadable form (called "ciphertext").\(^{21}\) Anyone who later obtains possession of the message will be unable to read it without first "decrypting" the message—by using a "key" or by breaking the code.

The principal involved is very similar to that of a combination lock on a safe. "If the lock is well designed so that a burglar cannot hear or feel its inner workings, a person who does not know the combination can open it only by dialing one set of numbers after another until it yields."\(^{22}\) This technique, called a "brute force" attack, is costly and time consuming.\(^{23}\)

There are several different types of cryptographic systems. For example, in "Shared Single Key" cryptography systems, the same key which encrypts the information can be used to decrypt it.\(^{24}\) However, in "Public Key" cryptography systems, there are separate keys—one to encrypt the data and one to decrypt it.\(^{25}\) Under a "Public Key" system, X can send a message to Y by looking up Y's public key in a directory and using that key to encrypt the data. Upon receipt, Y can decrypt the information using his/her secret private key.

The technical details of the various types of cryptographic systems are very complex and beyond the scope of this Note. At this point, all the reader needs to understand is that encryption can scramble information, thereby requiring individuals wishing to read the material to have the appropriate key or the power and time to perform a "brute force" attack.


\(^{23}\) Id.

\(^{24}\) Tanenbaum, supra note 20, at 581.

\(^{25}\) Id. at 581-582.
B. WHY IS ENCRYPTION NECESSARY ON THE INTERNET?

The world isn't run by weapons anymore, or energy, or money. It's run by ones and zeros—little bits of data. It's all electrons . . . There's a war out there, a world war. It's not about who has the most bullets. It's about who controls the information . . . It's all about information.  

As Cosmos, the villain in the movie *Sneakers*, states above, information is a source of power and money in today's society. Given the volume of data that individuals and businesses store and the fact that storage is much easier in an electronic format, computers have become modern day treasure troves.  

Hackers, the technology savvy criminals who are the pirates of the information age, often target these computer data banks. These attacks financially threaten individuals and businesses connected to the Internet, damage the growth potential of electronic commerce, and place people's lives in danger. This next section discusses some of these threats and how encryption serves to lessen the risks involved.

1. **Effecting Individual and Business Finances On-line.** Nobody knows exactly how much computer crime there really is. However, it is clear that the Internet and Cyberspace create a realm which is extremely lucrative for high-tech criminals. Given the size of the Internet, even small crimes may have large payoffs. For example, "'Salami slicing' . . . involves a thief who regularly makes electronic transfers of small change from thousands of accounts to his own. Most people don't balance their ledgers to the penny so the thief

---


27 In addition to the voluminous amount of trade secrets and other corporate information located online, there is an enormous amount of personal data contained by the government and various private sector organizations. George B. Trubow, *Protecting Informational Privacy in the Information Society*, 10 N. Ill. U. L. Rev. 521, 523. For example, the Department of Health, Education and Welfare, the Selective Service System, and the Internal Revenue Service all cross reference information through the use of social security numbers. *Id.* As a result, "anyone who knows an individual's SSN can amass a wealth of highly sensitive information about that individual." *Id.* at 526. See also infra notes 45-47 and accompanying text (discussing personal information on-line).
makes out, well, like a bandit."²² Another lucrative area for cyber-thieves encompasses stolen services. Bob Gibbs, a Financial Fraud Institute senior instructor, says that swiping and reselling long-distance calling codes is big business.²⁹

Businesses connected to the Internet are at the greatest risk. The Computer Security Institute (CSI) recently announced the results of its third annual "Computer Crime and Security Survey."³⁰ According to CSI, sixty-four percent of the respondents suffered from security breaches within the last year.³¹ Although seventy-two percent of these respondents acknowledged suffering financial losses, many of the victimized organizations were unable to estimate their losses.³² "The total financial losses for the 241 organizations [forty-six percent of the survey] that could put a dollar figure on [their loss] adds up to $136,822,000."³³

As startling as these numbers are, evidence suggests that piracy occurs even more frequently. First, many break-ins go undetected.³⁴ For example, in tests designed to evaluate the security of military data banks, the Defense Information Systems Agency ("DISA") successfully broke into ninety-five percent of the Department of Defense's ("DOD") unclassified computer systems.³⁵ Of these break-ins, only four percent were detected.³⁶ Given the military's four percent detection rate, the corresponding rate in the civilian world is arguably quite low.³⁷

²² Sussman, supra note 10, at ¶ 5.
²⁹ Id. at ¶ 6.
³⁰ Annual cost of computer crime rises alarmingly; Organizations report 136 million in losses (visited Mar. 20, 1998) [hereinafter Cost of Computer Crime] <http://www.gosci.com/prelea11.htm> (summarizing the report and offering a free copy to all interested parties). CSI conducts the survey with the help of the Federal Bureau of Investigations by soliciting "responses from 520 security practitioners in U.S. corporations, government agencies, financial institutions and universities." Id. at ¶ 3. See also M.J. Zuckerman, Cybercrime against business frequent, costly, USA TODAY, Nov. 21, 1996, at 1A ("Hackers and competitors broke into the computer systems of almost six of every 10 major U.S. corporations in the past year.")
³¹ Cost of Computer Crime, supra note 30, at ¶ 5.
³⁴ Goodman, supra note 7, at 475.
³⁷ Id.
Secondly, even those break-ins that are detected often are not reported. In a confidential survey conducted in conjunction with the Senate Permanent Subcommittee on Investigations, IBM, Security Dynamics and other major corporations, thirty seven percent of the companies did not want to involve the police and would report the crime only if required by law. Of these companies, nineteen percent justified their response by citing a "[c]oncern that the crime would become public" and eighteen percent feared "the loss of client confidence."

Although statistics are not as prevalent, the level of piracy worldwide is even more troublesome. In 1996, two leading international software associations reported the results of the first independent survey on global software piracy. The survey incorporated data from eighty countries during 1994 and 1995 and concluded that worldwide software piracy costs exceeded thirteen billion dollars in 1995.

As companies continue to expand their business operations around the world, there will be increasing pressure "to exchange sensitive information with—foreign branches, joint venture partners, subsidiaries, subcontractors, product suppliers, and customers . . ." and as such, the risk of stolen information will continue to increase. Encryption provides the lock that individuals and businesses need to protect the information which they store or transfer electronically. In fact, many people agree that the "best way to reduce many types of industrial and financial crime is to provide . . . powerful encryption [for use against] corporate spies and thieves." Essentially, encrypted information is not a very tempting target because any thief who obtains such information will be unable to read it without first breaking the code.

38 Zuckerman, supra note 30.
39 Id. at ¶ 7.
40 Id.
42 Id. at ¶ 3.
2. **Effecting the Growth of Electronic Commerce.** Reducing piracy is not only in the best interests of those businesses which are losing millions of dollars, but it is also vital for the growth and success of electronic commerce. Without a secure and trusted infrastructure, individuals are much less likely to move their private business or personal information on-line.\(^{45}\) The existence of a new trade—"Paid Internet Searcher"—suggests that the reluctance to go on-line is likely justified.\(^{46}\) Carole Lane, an "Internet Searcher" and author of *Naked in Cyberspace: How to Find Personal Information Online*, describes the availability of personal information in cyberspace, saying:

In a few hours, sitting at my computer, beginning with no more than your name and address, I can find out what you do for a living, the names and ages of your spouse and children, what kind of car you drive, the value of your house and how much taxes you pay on it.\(^{47}\)

Without encryption technology, online information will become even more vulnerable and individuals will become even more reluctant to place information on the Internet. This reluctance threatens to damage the growth of electronic commerce. The President of the Americans for Tax Reform has compared the scenario with the settling of the Wild West: if the government had refused individuals the right to lock their front doors or place a fence around their farms the "West would still be lawless."\(^{48}\)

---


\(^{47}\) Quittner, supra note 46, at 33.

\(^{48}\) Relaxing Limits on Export of Encryption Software: *Hearings on H.R. 695 Before the House Judiciary Comm.*, Mar. 20, 1997, available in 1997 WL 154158 (F.D.C.H.). See also, Blaze, supra note 22, at 1.1 ("The dirt paths of the middle ages only became highways of
3. Protecting Information in Order to Protect People. Undoubtedly, businesses have a strong interest in protecting the billions of dollars worth of information that is stored in computer banks; most people would agree that the continued growth of electronic commerce and the dream for a global economy are valuable goals. However, these financial justifications for the use of encryption pale in comparison to the tremendous role that encryption plays in protecting people’s lives.

“Air traffic control centers, electric-power grids, defense systems, financial services, oil and gas producers and suppliers, telecommunications networks and the stock market all operate and communicate by computer.”

If encryption were not used to limit access to such systems and to scramble all the data contained therein, people’s lives would be in serious danger. Consider the following scenario:

A hacker breaks into the computer systems at Brigham & Women’s Hospital at four o’clock on a Monday morning. Before most of the doctors arrive to treat their patients for the day, the malicious computer intruder changes a number of patient files on the hospital’s central database system: surgeries slated to be performed on the right leg are now switched to the left leg; recorded blood types are altered from AB-negative to O-positive; warnings for known allergies to medicines such as penicillin are electronically erased from patient’s charts; and laboratory records on HIV blood test results are insidiously switched from negative to positive just before patients are to receive their results.

By rendering the information in the hospital’s central data base unreadable, encryption protects against such attacks.

---

business and culture after the security of travelers and the merchandise they carried could be assured. So too the information superhighway will be an ill-traveled road unless information, the goods of the Information Age, can be moved, stored, bought, and sold securely.”.


60 Goodman, supra note 7, at 466.
4. **Summary.** In summary, there is an abundance of financial crime on the Internet and both individuals and businesses need encryption to protect information which is stored or transferred electronically. Furthermore, informational piracy is making consumers increasingly reluctant to place data on-line and the failure to use encryption technology to create a secure infrastructure for electronic commerce may place the growth of cyberspace in jeopardy. Lastly, our national infrastructure also depends upon the Internet. Unless encryption is utilized to limit access to the computers which run hospitals, traffic control centers, power grids, and defense systems, human lives may be at risk. All of these factors lead some individuals to the conclusion that encryption is a vital component of the information age.  

C. **WHY WOULD THE GOVERNMENT WANT TO LIMIT ENCRYPTION TECHNOLOGY (Policing Cyberspace)?**

Despite the fact that encryption has extremely valuable uses, it also has some serious drawbacks. The same technologies that allow consumers and businesses to scramble financial information, thereby diminishing the risk of piracy, can also help thieves commit different types of crimes. Illegal activities such as money laundering, fraud, stalking, gambling, terrorism, the commission of hate crimes, and the distribution of child pornography are all easier to accomplish when criminals are able to conceal their identities and the substance of their on-line transactions through the use of encryption.

---

61 Group Letter, supra note 45 (stating that encryption technologies are the "vital tools consumers and businesses need to operate with security and privacy in the information age, and are a cornerstone of electronic commerce").

62 Nicholas W. Allard & David A. Kass, *Law and Order in Cyberspace: Washington Report*, 19 HASTINGS & ENT. L.J. 563, 573 (1997) ("Law enforcement has realized that this same encryption technology [which prevents crime] can be used to conceal money laundering, other fraudulent or illegal transactions, or even espionage and terrorism."). See also, *FBI to parents: Internet pedophiles a serious threat* (visited Mar. 11, 1998) <http://cnn.com/TECH/computing/9803/11/cyber.stalking/index.html> (describing how an FBI agent pretending to be a teen-age girl signed on to a "chat room" in order to trap pedophiles. If the pedophiles identities were disguised with strong encryption, this police tactic would prove ineffective and children would be in danger). See also Goodman, supra note 7, at 465 (offering more descriptions of computer crime).
Quite simply, the government wants to limit the use of encryption for fear that law enforcement will be unable to use electronic surveillance to combat crime. As Louis Freeh, the Director of the Federal Bureau of Investigation ("FBI"), states, "Congress has on many occasions accepted the premise that the use of electronic surveillance is a tool of utmost importance in terrorism cases and in many criminal investigations, especially those involving serious and violent crime, terrorism, espionage, organized crime, drug-trafficking, corruption and fraud." 3

Indeed, the FBI provides many examples of situations where eavesdropping has been a key tool in law enforcement's successful attempts to stop crime. For example, terrorists in New York who were plotting to bomb the United Nations building were stopped and convicted due to evidence obtained by court-ordered electronic surveillance. 4 This type of electronic surveillance also played a crucial role in World War II, as the highly sophisticated signals intelligence (SIGINT) capability shortened the war and saved hundreds of thousands of lives. 5 As such, law enforcement justifiably wants to assure its surveillance capabilities. This desire leads the government's attack against the use of encryption. Indeed, the FBI claims that:

[T]he widespread use of robust unbreakable encryption ultimately will devastate our ability to fight crime and prevent terrorism [and] will allow drug lords, spies, terrorists and even violent gangs to communicate about their crimes and their conspiracies with impunity. We will lose one of the few remaining vulnerabilities of the worst criminals and terrorists upon which law enforcement depends to successfully investigate and often prevent the worst crimes. 6

---


54 Id.


56 Freeh, supra note 53, at ¶ 4.
To some, the above statement teeters on the borderline of propaganda. Drug lords, terrorists, violent gangs, it sounds as if Armageddon is coming. However, the government correctly notes that the structure of the Internet and the unique nature of Cyberspace both create serious problems for law enforcement agencies. This next section allows the reader to fully appreciate the complexity of the encryption debate by briefly articulating how law enforcement is already very difficult in Cyberspace and why the government is therefore concerned about the addition of more obstacles, such as the use of robust encryption.

1. The Internet and Interconnection. The interconnected nature of the Internet creates problems for law enforcement trying to track and convict criminals who commit their crimes on the Internet. First, cyberspace provides a maze in which the computer criminals can hide. Goodman points out that the Internet was "designed to survive a nuclear war and provide[s] innumerable pathways for messages to be sent; if one route [is] destroyed, the message ha[s] to be able to 'react' and find a new path to its intended destination."\(^{57}\) This architecture is well-suited for military command control operations but creates difficulties when it comes to limiting and tracing access to informational depositories in Cyberspace.\(^{58}\) In the digital world, any given information located on a computer server is "connected to dozens, hundreds or even thousands of other computer systems around the world."\(^{59}\) This web results in an infinite number of possible paths which hackers could follow to infiltrate a given data bank. As such, hackers can "cover their tracks by 'looping and weaving' in and out of dozens of computer systems around the world, masquerading as legitimate users on the co-opted system."\(^{60}\) Hence, law enforcement encounters a major obstacle trying to track criminals on the Internet.

Second, the Internet is global,\(^ {61}\) allowing for criminals to commit crime in one country while located in another. Such activity

\(^{57}\) Goodman, supra note 7, at 483.
\(^{58}\) Id.
\(^{59}\) Id. at 471.
\(^{60}\) Id. at 483.
\(^{61}\) See Intel to focus on networks, supra note 17 (noting that there will soon be a billion connections to the Internet).
CRYPTOGRAPHY

creates further problems relating to jurisdiction and extradition.62

2. The Problem with Cyber-evidence. Another complication pertaining to the policing of cyber-crime stems from the difficulty of obtaining digital evidence. As noted earlier, Cyberspace consists of electronic bits which basically have no size or weight.63 As such, the payoff of any given computer crime often can be stored on a small disk.64 Unlike criminals who rob a bank or an armored car of two million dollars in cash and face serious difficulties storing and transporting the fruit of the crime, the cyber-criminal can fit the stolen goods into his/her pocket.65 If the evidence can also be encrypted so as to be nearly unreadable, law enforcement argues that they may never be able to collect the necessary evidence to convict a cyber-criminal.

3. Summary. The inherent difficulties of preventing crime in cyberspace which stem from the interconnected nature of the Internet and the difficulty of obtaining digital evidence create serious obstacles for law enforcement.66 Although some crime can be stopped by business and consumer use of cryptography,67 such use cannot stop every type of crime. Hence, the government is very concerned with the widespread use of encryption and feels that the use of this technology should be somewhat limited.

IV. THE PRAGMATIC DEBATE OVER THE PROPOSED SOLUTION— IS "KEY RECOVERY" REALLY THE KEY?

Considering the strong need for encryption and all of the law enforcement problems this technology creates, the government is

63 See discussion infra Section II.A.
64 Goodman, supra note 7, at 471-72.
65 Id. at 472.
66 See, Dorothy E. Denning, Statement Before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism, and Government Information (visited Dec. 5, 1997) <http://guru.cosc.georgetown.edu/~d...crypto/Denning-Baugh-Testimony.txt> (reporting that law enforcement is having increasing problems because of criminal use of encryption. The report was based on responses to a questionnaire which was sent to listed members of the High Tech Crime Investigations Association and the G-Two-I intelligence list).
67 See supra Section III.B. for a discussion on the benefits of encryption with respect to protecting against certain types of financial crime on the Internet.
faced with three basic courses of action. First, the government could decide to do nothing. Individuals would have access to the strongest encryption available. This approach would result in a decrease in certain crimes committed on the Internet—mainly the piracy of valuable information. However, criminals would also have access to strong encryption, and this access might interfere with government surveillance designed to catch terrorists, money launderers, and other criminals.

Second, the government could try to curtail the use of all strong encryption. Even if this action is constitutional, which it may not be, the government would be threatening the future growth and use of the Internet. Without strong encryption, data sent on the Internet would be “no more secure than a postcard,” and few individuals or businesses would continue to operate under such conditions.

Instead of following these two paths, the government has chosen the “middle path between banning and deregulating strong encryption.” This approach has been labeled “key recovery.” This next section briefly describes the “key recovery” and some of the pragmatic arguments which opponents have marshaled against the government’s proposal.

A. WHAT IS “KEY RECOVERY”? 

Essentially, the government is attempting to resolve the encryption debate by allowing the use of strong encryption technologies if there is a built-in “key recovery” mechanism which will guarantee law enforcement access to the plaintext.

There are numerous types of “key recovery” systems, and a detailed description of them is beyond the scope of this Note.
Although these systems differ, the basic concept is the same. In order to understand the debate, all the reader needs to know is that any "key recovery" system has two essential elements: (1) "A mechanism, external to the primary means of encryption and decryption, by which a third party [i.e. the government] can obtain covert access to the plaintext of the encrypted data;"\(^7\) (2) "The existence of a highly sensitive secret key (or collection of keys) that must be secured for an extended period of time."\(^8\)

Basically, companies and individuals would be able to use strong encryption as long as the cryptographic system also provided a "key" that could decrypt the information without the knowledge of the sender or recipient. The government or some third party would then hold the key in escrow until law enforcement could demonstrate a valid need for the key.\(^9\)

B. PRAGMATIC ARGUMENTS AGAINST "KEY RECOVERY"

The Internet community has joined to oppose any "key recovery" system and has compared the proposal to the FBI's demanding "a front door key to every American's house, just in case a criminal happens to be hiding out somewhere."\(^10\) This section of the Note summarizes the various pragmatic arguments that opponents of the proposed legislation have marshaled against "key recovery." The first set of arguments declare that "key recovery" is doomed to fail. The second set of arguments proclaims that, given the likelihood that any attempt at "key recovery" will fail, it would be unwise to attempt the creation of such an infrastructure because its costs would be enormous.

1. **Imminent Doom of "Key Recovery."** Most opponents of "key recovery" argue that the system is very likely to fail. First, critics argue that it would be technologically infeasible to build the infrastructure that the new legislation would require to operate a successful "key recovery" scheme. Leading cryptographers and

\(^{7}\) Id. at § 1.2.

\(^{8}\) Id.


\(^{10}\) Bill Pietrucha, **ACLU Calls Encryption Actions Nightmare For Privacy**, NEWSBYTES NEWS NETWORK, Sept. 12, 1997, available in 1997 WL 13910671.
computer scientists agree that "[b]uilding a secure infrastructure of the breathtaking scale and complexity demanded by these requirements is far beyond the experience and current competency in the field." As Matthew Blaze, a principal research scientist at AT&T Research notes, "[i]t is not clear that key [recovery] makes any sense from a technical perspective . . . Encryption is very fragile . . . [and] it is a rather naive view to assume we can design a key [recovery] system securely any time soon."79

Secondly, opponents of key recovery systems argue that even if the necessary infrastructure can be built, it will prove ineffective because "[c]riminals and terrorist groups will not use a system that gives the government access to their decryption keys."80 Quite simply, a criminal would not choose software "that happens to have a way in for Uncle Sam" when other encryption technologies are available.81

The FBI counters this argument by pointing out that criminals and terrorists still use telephone corporations even though it is common knowledge that the government can, under proper authority, eavesdrop on the conversations.82 However, a criminal wishing to place a phone call within the United States has a limited number of choices with respect to service providers. Transactions occurring on the Internet can be guarded with encryption products obtained from anywhere in the world.83 As such, there is a strong argument that many criminals will not use "key recovery" cryptographic systems.


80 Group Letter, supra note 45 (noting that "the FBI has admitted in Congressional testimony that criminals will always have access to strong, unbreakable encryption").

81 William J. Cook, Scrambled Signals From Washington: The Clinton administration wants to help companies (without hurting America’s spies), U.S. NEWS ONLINE, ¶ 8 (Nov. 14, 1996) <http://www.usnews.com/usnews/issue/14SOFT.htm> (noting that "neither NTT in Japan nor British Telecom are required by their governments to maintain keys").


2. The Costs of Attempting to Build a "Key Recovery" Infrastructure. As described above, there is some indication that any attempt at establishing a "key recovery" system would be imminently futile. In addition, it would be extremely costly to try to create such a system.

First, there is evidence from the Information Technology Association of America that because of current restrictions, "American companies could lose up to 65 billion dollars ($65,000,000,000) in the export market for cryptography by the end of the decade." As described earlier, requiring "key recovery" will likely result in even more lost business for American companies, since foreign consumers will be less likely to buy encryption products which contain a way in for the U.S. government.

Secondly, there is fear that by providing a "back door for police," "key recovery" systems will introduce a new path to the information and result in less secure systems. In fact, many opponents of "key recovery" describe the external means of decryption provided by the key as a "trap door" and are fearful that hackers will utilize the path to decrypt sensitive information.

Lastly, the "key recovery" system will require storage of highly sensitive keys. These storehouses will become prime targets for sophisticated hackers. Given the prevalence of break-ins into corporate and military systems and the government's poor record of detection, some individuals feel that it would be extremely unwise to keep keys in electronic storage.

---

84 S.J. Res. 29, 105th Cong. (1997) (relating to repealing export restrictions on encryption software and hardware products). But see, Reinsch, supra note 82, at ¶ 16 ("Commerce and NSA studied the foreign availability of encryption in 1995, and . . . did not find that claims of widespread foreign availability of encryption products were accurate.").

85 See discussion infra section IV.B.2.

86 Abelson, supra note 45, at ¶ 3.1.

87 Group Letter, supra note 45, at ¶ 3 ("mandating trap doors in all domestic encryption products and communication networks . . . will make the personal records and communications of individuals and businesses more vulnerable to hackers, terrorists, industrial spies and other criminals.").

88 Abelson, supra note 45, at ¶ 3.1.3.

89 See discussion infra Section III.B.1 (describing the prevalence of break-ins and the low detection rate of the government). See also, Social Security officials insist Web info is secure (Apr. 8, 1997) <http://cnn.com/TECH/9704/08/soc.sec.internet/index.html> (noting that officials insist that social security records located on the net are secure despite the fact that a graduate student took only three and one-half hours to crack a code which was very similar
3. Summary. Hence, attempting to create a “key recovery” infrastructure could cost U.S. computer companies millions of dollars, result in less secure encryption (because of another path to the plaintext), and render very valuable data storehouses open to attack. It is extremely unwise to accept these risks given the doubt that a satisfactory system can be built and the low probability that criminals will use a “key recovery” system.

V. A THEORETICAL ARGUMENT AGAINST “KEY RECOVERY”—THE ELIMINATION OF PHYSICAL BARRIERS AND THE INEFFICIENCY OF LEGAL CONSTRAINTS

The aforementioned arguments against the use of “key recovery” are very practical and quite convincing. Nonetheless, there is another strong critique of the proposed “key recovery” system which is more theoretical. This section of the Note asks the reader to consider the future of our society and the effect that “key recovery” legislation may have on that future.

This Note argues that both physical and legal limits are necessary to keep the government in check and protect the freedom of individual citizens. Allowing the government to obtain keys for decrypting codes would be equivalent to breaking down Cyberspace’s physical limitations on government surveillance. Providing legal restraints on law enforcement agencies is not enough,60 as legal limits by themselves will prove insufficient to protect individual privacy.

Part A of this section describes how the physical limitations of Cyberspace differ from the natural limits in the real world. Part B describes how “key recovery” could practically eliminate all physical boundaries on government surveillance. Finally, part C examines how the law has struggled to protect privacy whenever technological advances eliminate physical barriers.

---

60 One example of a purely legal constraint is a requirement that law enforcement agencies obtain a valid court order before encryption keys are released to the government.
These observations lead to the conclusion that providing the government with "key recovery" and thereby eliminating the natural physical barrier of encryption that has evolved as Cyberspace has developed, would be extremely unwise. Although legal limitations can be utilized to curtail the government's ability to decrypt messages and spy on citizen transactions on-line, legal limits alone are not enough.

A. HOW THE BARRIERS OF CYBERSPACE DIFFER FROM THE BARRIERS IN THE REAL WORLD (NATURE VS. CODE)

This section posits that the constraints limiting activity in Cyberspace are qualitatively different from the constraints limiting activity in the real world (also described as "real space"). This difference needs to be taken into account when discussing encryption and "key recovery" legislation.

1. Constraints in Real Space. The law is just one constraint which regulates real space. The law tells people not to take an object from a store without paying for it, not to drive faster than a designated speed on the highway, and not to enter someone's house without permission.

Nature also regulates behavior in real space. For example, "[t]hat I can not see through walls is a constraint on my ability to snoop. That I can not read your mind is a constraint on my ability to know whether you are telling me the truth. That I can not lift large objects is a constraint on my ability to steal." In this way, nature regulates behavior.

However, nature and law constrain differently. The law constrains by ex poste punishment. To a large extent, individuals choose whether to steal or not. If they do steal, then they run the risk of conviction and punishment. Nature regulates much more directly. "One doesn't choose not to see through a brick wall for fear of punishment that nature will visit upon such an infrac-

---

92 Id.
93 Id. Note the importance of choice, as evidenced by the prevalence of speeding.
94 Id.
2. *Constraints in Cyberspace.* Cyberspace also has various constraints which regulate behavior. For example, copyright, defamation, and obscenity laws all “threaten ex poste sanction for the violation of some legal right.”

The Cyberspace equivalent of nature is the computer code which defines the operations occurring on the Internet. “The code, or the software that makes cyberspace as it is, constitutes a set of constraints on how one can behave in cyberspace.” For example, an individual cannot log on to certain networks without entering his/her password. Similarly, someone cannot intercept and read a message which has been encrypted unless he/she has the key or is able to break the code. Just as nature directly regulates real space, computer code directly regulates Cyberspace. One cannot choose to enter America Online without a password any easier than one can choose to see through walls.

3. *An Important Difference.* Hence, Cyberspace is much like real space—both contain legal and physical constraints. However, the code of Cyberspace is much more plastic than the natural barriers of real space. As such, legislation (like “key recovery” proposals) which attempts to regulate the code utilized on the Internet should be viewed as trying to define the physical limits of Cyberspace.

B. KEY RECOVERY AND ITS EFFECT ON THE PHYSICAL LIMITATIONS OF CYBERSPACE

“Key recovery” legislation mandates that all encryption systems be written in a certain way (i.e. allowing for third-party access) and therefore will operate as a control of the future code in Cyberspace. This section argues that this code change will greatly diminish current physical limitations on government surveillance.

1. *Current Limitations in Real Space.* Before one can understand how “key recovery” would increase the government’s surveillance capabilities, it is important to understand what power the government currently has in real space. Currently:

---

95 Lessig, *supra* note 91, at 183.
96 Id.
97 Although hackers can break into America Online without a password, infra-red technology allows people to see through walls. However, both of these techniques are exceptions rather than the norm.
If the government wants to read your mail, it has to sort through trillions of physical pieces of paper that might be anywhere in the country. This is difficult, time consuming, and expensive.\footnote{Hearings on H.R. 695, supra note 48, at 4.}

If the government wants to listen to your phone calls, [it must] pay people to listen, and listening takes a long time. Even though you can electronically sort out telephone calls . . . technology is such that you still have to hire people to listen, and this again is expensive.\footnote{Id.}

The government cannot easily monitor . . . groups of people that meet in three dimensional space—like your church, your business, or your local bar.\footnote{Id.}

The government cannot easily track what you do with physical currency.\footnote{Id.}

2. Cyberspace Surveillance. Cyberspace is popular precisely because it lacks many of the physical barriers present in the “real space.” Internet users can skip from a web site in California to a web site in Germany; and the computer can search thousands of records per second for a particular key word.

Luckily, encryption has evolved as Cyberspace developed and provides some physical limitations on government surveillance. Quite simply, the government must expend computer time and energy in order to break codes and read information available online.\footnote{Id.} If the government had a key to the code, it would be unnecessary to expend the energy. As such, the government would have unprecedented ability to gather all sorts of information. In order to help the reader better appreciate this risk, the following paragraphs describe some of the technology which already exists for “big-brother” type surveillance and the immense power of government computers.

The technology already exists for unprecedented surveillance. For example, programs called “sniffers” can be commanded to look
for signals of any sort. In 1992, a twenty-year-old schizophrenic boy named Matt Singer used his personal computer and a sniffer program to accumulate hundreds of thousands of passwords and account names. By working diligently for about three months, Singer managed to install sniffers on the major backbones of the Internet. With these sniffers, Matt managed to accumulate enough information to break into “classified military sites, nuclear-weapons labs, bank ATM systems, Fortune 100 companies, [and] dam control systems.” If a boy on a home computer can accumulate that much data, then imagine the amount of information the government could obtain with its computer resources if it did not have to exert energy breaking encryption codes.

The government already has the world’s fastest computer—an Intel ASCI Red Unit designed to perform one and one-half trillion operations per second and has recently awarded a four and one-half million dollar contract to lease computer time at the Pittsburgh Supercomputing center. The government may “set up systems so fast that they could do 30 trillion calculations per second by 2001—and 100 trillion by 2004.”

In addition to programs (like sniffers) that collect information traveling through Cyberspace, the government has access to

---

103 See David H. Freedman & Charles C. Mann, Cracker: This computer geek could have taken down the networks of military sites, nuclear-weapons labs, Fortune 100 companies, and scores of other institutions. It might have been partly your fault, U.S. NEWS ONLINE, ¶ 28-34 (June 2, 1997) [http://www.usnews.com/usnewsissue/97060212CRAC.HTM] (discussing how sniffers can be used to look for key words such as “merger” or “proxy” to screen for financial transactions).

104 Id. at ¶ 28-35.

105 Id. at ¶ 915.

106 Id. at ¶ 127.

107 Energy Department taps into powerful academic computers (Mar. 9, 1998) [http://cnn.com/TECH/computing/97030909/nuke_computers.ap/index.html] [hereinafter Powerful Academic Computers]. See also, Douglas Waller, Spies in Cyberspace, TIME, Mar. 20, 1995, at 63-64 (noting that the CIA’s “computer system at Langley stores more than 4 trillion bytes of information—equal to a stack of documents 30 miles high. Its computer-disk farms, which take up two floors the area of two football fields, have numbers and letters painted on the walls, like a parking lot, so technicians don’t get lost in the mainframes.”).

108 Powerful Academic Computers, supra note 107, at ¶ 1.
programs which can infiltrate a given system that is connected to the Internet. One example is a “worm.” “[A] ‘worm’ is a program that travels from one computer to another but does not attach itself to the operating system of the computer that it ‘infects.’” In the fall of 1988, a first-year graduate student in Cornell University’s computer science Ph.D. program wrote a computer program of this nature in order to “demonstrate the inadequacies of current security measures on computer networks.” Because of a miscalculation, the worm replicated much faster than had been anticipated and eventually caused many computers to shut down, including computers relied upon by various universities, military sites, and medical research centers. Considering the large number of computers that Morris was able to infect with one worm program released from a single computer, it is staggering to imagine how many computers the U.S. government could infiltrate with its high power computers. Now consider the fact that a “worm” could theoretically be programmed to enter into thousands of computer systems and look for specified information. The ease with which the government could monitor all material and transactions on-line is frightening.

110 Id. at 505.
111 In order to prevent the worm from copying itself onto a computer that already had a copy (an event that would cause the computer system to bog down and crash), Morris had the worm “ask” each computer whether there was an existing copy of the worm. Morris, 928 F.2d at 506. If the response was “no,” then the worm copied itself onto the computer; if the response was “yes,” the worm was not duplicated. Id. To stop other programmers from killing the worm by programming their computers to provide false “yes” responses, Morris programmed the worm for automatic duplication upon every seventh “yes” response. Id. Since Morris underestimated the frequency with which a computer would be asked the question, his automatic duplication ratio was incorrect and the worm copied itself far more often than Morris had intended. Id.
112 Id. at 506.
113 Id. at 505 (Morris used a computer from the Massachusetts Institute of Technology to release the worm in order to disguise the fact that he released the worm). Id. at 506.
114 See Michael Adler, Note, Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search, 105 YALE L.J. 1093, 1098-99 (1996) (discussing a hypothetical government search program that could be used to detect digital contraband).
C. LEGAL LIMITS ARE NOT SUFFICIENT

It is true that some "key recovery" legislation provides legal limitations on the government's ability to obtain the keys.\(^{115}\) Most people put great faith in these legal limitations. Indeed, our complex system of legal rights and duties provides the necessary order for our civilized society by facilitating interaction between citizens and by maintaining a proper balance between individual rights and the government power necessary to protect those rights. Optimism demands that we feel confident in the ability of our laws to maintain this structure. This Note was not written in order to destroy the feeling of security that our constitutional rights provide. Rather, the purpose of this Note is to demonstrate that these legal boundaries are insufficient alone to maintain the necessary balance between individual rights and governmental control. Instead, the combination of legal and physical limitations on the government maintains this necessary balance.\(^{116}\)

Past experience has demonstrated that legal limits often prove inadequate when physical limitations are eliminated. This section examines the Fourth Amendment and how courts have struggled to give it full effect whenever technological advances have allowed for law enforcement to circumvent a physical limitation on government surveillance—focusing on wire-taps, infra-red surveillance technology, and Millivision. Given that legal limits have particular problems when physical barriers are removed, this Note advises against "key recovery."

1. Wire-Tapping Technology—Breaking Down Physical Barriers and Reformulating the Right to Privacy From a Property-Based Regime to an "Expectations" Regime. Earlier this century, the United States Supreme Court utilized a property-based analysis for Fourth Amendment questions. Essentially, the government could only confiscate property in which it had a superior possessory interest. Under this approach, "[courts would not conclude that a search and seizure had even taken place unless the government

\(^{115}\) The Risks of Key Recovery, supra note 76.

\(^{116}\) The government could not possibly follow every other person around and listen to all their conversations. Note, however, that it would be theoretically possible to listen in on every third conversation on the Internet if encryption codes were ineffective.
infringed a property interest." This analysis also applied to investigative techniques which were declared unconstitutional as a violation of the Fourth Amendment only if the technique infringed upon a property right.

This bright line rule helped the property-based paradigm function quite efficiently, until technological advances began destroying some of the physical boundaries. Wire-tapping equipment enabled the government to listen in on phone conversations without physically entering the suspects' property. For example, in *Olmstead v. United States*, the government used wire-taps to listen in on various phone conversations of individuals who were suspected of breaking prohibition laws. Since the wire-taps were placed on the phone lines leading into the suspects' houses, the Court held that there was not an unreasonable search and seizure. The Court explained that, "[t]he language of the Amendment can not be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office."

The property-based Fourth Amendment analysis resulted in similar conclusions when the government used other listening devices. In *Goldman v. United States*, the government placed a detectaphone outside the wall of a room where the defendant was making telephone calls. Since this manner of monitoring phone calls did not encroach onto the suspect's property, the court held the search to be consistent with the Fourth Amendment.

As technological advances continued to break down physical barriers and allowed government surveillance without an encroachment on property rights, the Court was forced to reassess the

---


118 Id. at 55.

119 277 U.S. 438 (1928).

120 Id. at 464-65.

121 Id. at 465.

122 316 U.S. 129 (1942).

123 Id. at 135; *see also* Silverman v. United States, 365 U.S. 505, 506-09 (1961) (holding a search to be in violation of the Fourth Amendment only because the "spike mike" used to eavesdrop on defendant's conversation actually touched his premises).
Fourth Amendment doctrine. The new test involved an assessment of the suspect’s "reasonable expectation of privacy." In *Katz v. United States*, law enforcement officials attached an electronic listening device outside a public telephone booth in order to catch the defendant placing interstate gambling calls. Using the same property-based Fourth Amendment analysis as in *Olmstead*, the court of appeals affirmed the conviction. The Supreme Court reversed, holding that the Fourth Amendment protects people rather than places. The Court articulated a new test, stating that there was a violation of the Fourth Amendment because of the expectation of privacy that individuals usually attach to their conversations in phone booths. Thus, the test became whether an individual had an expectation of privacy that society was willing to recognize as reasonable.

As technological advances broke down traditional physical limitations on eavesdropping, the Court needed to change the property-based Fourth Amendment test to an expectation-based test. This change appeared to solve the problem for the time being.

2. What is a Reasonable Expectation of Privacy: Infra-red and Electromagnetic Detection Devices—The Elimination of Physical Barriers Resulting in a Struggle to Define the Fourth Amendment. The expectation-based Fourth Amendment analysis provided more protection against the wire-tapping surveillance of the government than did the property-based doctrine. Unfortunately, the new test has proven to be inaccurate in light of increasing technology. Expectations are not static; rather, they "change in the face of new technologies, such as DNA blood testing or weapons detection." Indeed, how reasonable is any expectation of privacy today when every citizen agrees to have a social security number, files detailed descriptions of spending habits on tax forms, and completes various

---

124 See, Krent, supra note 117, at 56 ("In an era of electronic eavesdropping and forensic laboratory testing, property no longer seemed a satisfactory proxy for the individual rights at stake.").
125 Id. at 58-59.
128 Katz, 389 U.S. at 351.
129 Id. at 353.
130 Id.
131 Krent, supra note 117, at 62.
other forms for the record? In light of the changing technology, the Court has struggled to define what is or is not a "reasonable expectation of privacy." During this struggle, a new standard called the "intimate details" test may be arising.\textsuperscript{132}

For example, consider whether individuals have a reasonable expectation of privacy from aerial surveillance. The Court has considered this question several times.\textsuperscript{133} In its Fourth Amendment examination, the Court appeared to focus on whether the surveillance revealed any "intimate details" of an individual's life.\textsuperscript{134} The first time a majority explicitly used the "intimate details" terminology was in Dow Chemical Co. \textit{v.} United States.\textsuperscript{135} There, Dow's industrial complex was photographed by an EPA aircraft using very expensive precision cameras. Although Dow had developed an "elaborate" security system, it did not conceal all of its equipment from aerial view. The Court held there was no search for Fourth Amendment purposes because "the intimate activities associated with family privacy and the home and its curtilage simply do not reach the outdoor areas or spaces between structures and buildings of a manufacturing plant."\textsuperscript{136} The Court used similar reasoning in other cases to hold aerial observation to be consistent with the Fourth Amendment as long as it did not reveal any intimate details.\textsuperscript{137}

Although the Supreme Court has not explicitly adopted an "intimate details" standard, lower circuit courts have noticed the Court's terminology and have used it when examining the constitu-

\textsuperscript{132} See, Merrick D. Bernstein, "Intimate Details": A Troubling New Fourth Amendment Standard for Government Surveillance Techniques, 46 DUKE L.J. 575 (providing a thorough analysis of the use of this terminology by the U.S. Supreme Court and how the lower federal courts began using it as a test.).


\textsuperscript{134} See, Bernstein, supra note 132 (summarizing the Supreme Court's use of this terminology).

\textsuperscript{135} 476 U.S. 227 (1986).

\textsuperscript{136} Id. at 236 (emphasis added).

\textsuperscript{137} See Ciraolo, 476 U.S. at 215 (acknowledging in the footnote that "aerial observation of curtilage may become invasive ... through modern technology which discloses to the senses those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens.") (emphasis added). See also, Riley, 488 U.S. at 452 (upholding the constitutionality of a law enforcement officer's observation, from an altitude of four hundred feet, of the interior of a partially covered greenhouse in a residential backyard).
tionality of the newest government surveillance tactics. For example, the Drug Enforcement Agency (DEA) and state police have used thermal imagery to convict drug abusers. Thermal imagery uses infrared detection to produce a visual image of an object based on the heat which it radiates. A screen then shows various colors, which correspond to the amount of heat produced, in slightly less detail than a television. The device does not project any beams or physically penetrate the objects targeted, and the infrared waves are not visible to the naked eye. By placing thermal imaging systems in airborne surveillance vehicles, the government can survey vast areas for “hot spots” characteristic of the high intensity lamps used for indoor growing of marijuana. The five circuit courts which have addressed whether the use of this device constitutes a search for Fourth Amendment purposes have all upheld the search as constitutional. Quite simply, there is no “search” under the “intimate details” standard unless intimate details are observed.

This test has been criticized as “an inquiry ex post into the content of the information revealed by surveillance—instead of the manner in which the information has been obtained.” Regardless of whether the standard is appropriate or not, the key point for this Note is that legal boundaries are struggling as modern technological advances call into question the concept of what constitutes a reasonable expectation of privacy.

Even if the “intimate details” standard was adopted, the technological advance known as “Millivision” may raise doubts about the effectiveness of that standard. “Millivision” uses passive imaging technology to read electromagnetic radiation emitted by an object. This data is utilized by “image understanding software” to convert the radiation data into a visual image similar to an x-ray. So far, a Fourth Amendment analysis of Millivision would not appear to be any different than one of thermal imagery. The key difference between the two technologies is the software which translates the information into the picture on the screen. With

138 Bernstein, supra note 132, at 588.
139 Id. at 589.
140 Id. at 586, n.104.
141 Id. at 577-78.
142 Id. at 600.
Millivision, the government can use “smart software” to recognize certain shapes such as dry powders in plastic bags. Moreover, Millivision can be programmed not to display any information unless it detects an item which the particular program has deemed to be “suspicious.” Therefore, it is possible to run a particular program so that Millivision automatically complies with the “intimate details” test used by the federal circuit courts for infrared government surveillance. Thus, the government could theoretically use Millivision to survey all activity and no one’s Fourth Amendment rights would be violated because no “intimate details” would be displayed on the screen.

How the Court will protect the right to privacy as technology continues to change the boundaries of possibilities is not exactly clear. What is clear is that legal limitations often struggle to keep pace with the exponential advancement of technology. Given this struggle, a “key recovery” system should not be used. Such a system would eliminate one of the few physical obstacles that Cyberspace provides against government surveillance and replace that physical limitation with a legal constraint.

VI. CONCLUSION

Determining whether or not to pass “key recovery” legislation is one of the most important decisions the legislature will ever make. Almost everyone who is close to the debate is aware that the decision will impact the financial well-being of businesses and individuals in the on-line community, shape the future of electronic commerce, and help determine how much success the government will or will not have against cyber-criminals.

Despite the importance of these effects, they pale in comparison to the real issue. The decision regarding key recovery is monumental because it will shape the very nature of Cyberspace. “Key recovery” legislation will result in an infrastructure of incredible proportions and will shape the protocol of the Internet. If the government is successful, all encryption programs will have “key recovery” systems. Such a scenario will allow the government to have unprecedented surveillance capability. Thus, the author

143 Id. at 602.
hopes that everyone involved in the encryption debate understands the importance of this decision.

KENNETH P. WEINBERG