NationalSecurityAgency

InformationAssuranceResearchGroup

(U)PRIVACY AND ANONYMITY

A TECHNOLOGY FORECAST

29 October 2002

(U) PRIVACY AND ANONYMITY

A TECHNOLOGY FORECAST

Table of Contents

(U) Preface

(U) The Technology Forecasting Program was implemented in accordance with NCS 21, Goals 1 and 2, and the National Security Agency's Corporate Plan for Information Assurance, Goal 6, to anticipate the impact of advancing technologies on NSA's mission. Forecasting and informational requirements are solicited from the Signals Intelligence Directorate, Information Assurance Directorate, and research organizations on significant information and communications technologies that will be used extensively within the next three to five years.

(U) Under the program, the Technology Assessment, Forecasting, and Transfer Office within the Research Associate Directorate, with the support of Honeywell Technology Solutions, produces a series of technology forecasts that assess emerging technologies, describe potential impacts, and guide the development of responsive investment plans. Using the evolving forecasting methodology, data is analyzed that is obtained from major marketing research companies from academia, industry, and government technical experts. Additional materials are collected through the review of technical periodicals and on-going community research activities. For additional information on the forecasting program, contact [redacted] Specific questions regarding this forecast should be directed to the author on [redacted]

(b)(3)-P.L. 86-36

By William J. Sonntag
Honeywell
Technology Solutions, Inc.

(U) Executive Summary

(U) One of the most contentious domestic debates since the dawn of the Internet Age, and especially since 11 September 2001, has been the controversy over how far an individual's right to privacy extends. Few U.S. social issues have generated as much legislative activity in recent years, particularly with reference to personal data found in e-mail and on the Internet. Although there is no explicit mention of privacy in the Constitution, many Americans regard it as much an inalienable right as freedom of speech and religion, and consequently our political leaders have felt compelled to respond. The Financial Services Modernization Act of 1996 (Gramm-Leach-Bliley Act), and Health Insurance Portability and Accounting Act (HIPAA) of 1999, and even the 9/11-conscious 2001 PATRIOT Act to a much lesser degree, are notable examples of U.S. statutes with privacy-protection provisions. In addition, concern about the proper balance between privacy and security has given rise in the summer of 2002 to introduction of legislation calling for a study of the best way to protect both. A major factor in the legislative call for a commission to conduct this study is the emergence of new technology-based surveillance devices.

(U) Privacy concerns and uncertainty about how to balance security and privacy are not uniquely American problems. Around the world, legislatures--most notably European--have taken action to ward off invasive attacks on the privacy of their citizens, all the while keeping in mind the threat of terrorism. An attempt in Britain's Parliament to extend surveillance powers granted by legislation 2 years ago was defeated in June 2002. Only weeks earlier, on the other hand, the European Parliament approved the Communications Data Protection Directive which grants authorities access to e-mail and Internet data for purposes of thwarting terrorism. Now the directive must receive the approval of the 15 member states of the European Union (EU), an uncertain outcome. Whatever the fate of this new directive, the EU has already established its credentials as a protector of its citizens privacy. The EU Privacy Directive of 1995 is regarded by many as a model for the rest of the world to follow, notwithstanding the misgivings of many in U.S. business and government circles about its effects on American commercial interests.

(U) Both governmental and non-governmental entities are contending with unprecedented threats to the security of their computers and communications, resulting in part from a gap created by escalating technology advances occurring without commensurate strides in security. Privacy concerns in both the public and private sectors have grown in large measure as a result of this dramatic progress. Conversely, anxiety about privacy and anonymity has also impacted technology, leading to development of new devices and protocols. New technologies and derivative devices have been viewed both as opportunity and threat. As advances beget vulnerabilities, individuals and businesses, as well as educational, health, and government institutions have all experienced some ambivalence, brought on by the potential for technology to assist in attainment of a salutary goal, while in some instances threatening to deprive the beneficiaries of privacy.

(U) For example, Palladium, a Microsoft initiative featuring a new encryption standard and touted by the company as providing increased security and privacy, is criticized by detractors as actually threatening privacy because hardware keys will be stored on a motherboard that would facilitate its identification. In addition, Microsoft's earlier Passport product with its convenient single sign-on feature purportedly was to keep personal information private, but has been found

lacking in this regard by the Federal Trade Commission. These and other technologies with privacy implications, including the Wi-Fi (Wireless Fidelity)/802.11 standard, Secure Socket Layer (SSL), PKI, Virtual Private Network (VPN), Platform for Privacy Preferences (P3P), Intrusion Detection Systems (IDS), and Biometrics will be discussed in this paper.

(U) Some civil libertarians, pessimistic about the current state of electronic privacy and technology's failure to guarantee it, believe strongly that anonymity is a major component of a solution. Anonymous remailers and browsing anonymizers have been promoted as invaluable tools in achieving this end. Nevertheless, most existing anonymity protocols are not an insurmountable obstacle to someone determined to acquire a user's identity. Even the highly regarded SafeWeb's anonymizing technology has been shown to be insecure. Not yet subjected to the rigorous review which SafeWeb technology has received, a new P2P anonymity protocol, Six/Four (refers to the 4 June 1989 Tienanmen Square massacre), was unveiled in the summer of 2002. Like most anonymity tools, it is already controversial because of its potential for illegal or other improper use.

(U) When IT privacy vulnerabilities become apparent, these become a force for development of technologies to address the problem. Deep concern in the United States and abroad will continue to be a major impetus in the generation of technologies designed to thwart privacy and anonymity threats. Nevertheless, there is growing awareness that a technology approach by itself will not solve the privacy problem. Although vigilance and proper use of existing privacy-protection measures, as well as development of new technologies, can handle many threats, pressure from users on their legislators needs to be applied for passage of laws to defend against unscrupulous parties taking advantage of the latest vulnerabilities.

(U//~~FOUO~~) NSA and other intelligence agencies have not been immune from the dilemma stemming from the need to respect others' (and protect their own) privacy, on the one hand, and maintain the nation's security with surveillance measures that may be intrusive, on the other. DIRNSA surfaced this issue when he appeared before the Congressional Joint Inquiry Committee on 17 October 2002. The Agency also experiences ambivalence with respect to protection of its anonymity, which is absolutely vital to certain aspects of its mission, but which is freely surrendered when accounts of historically significant SIGINT successes (e.g., VENONA program) are released publicly. Since NSA was created by Executive Order in 1952 and given its SIGINT and COMSEC missions, it has struggled to maintain its own privacy and anonymity, while attacking those of validated foreign targets, an undertaking which has been sanctioned by all three branches of Government as essential for the national security.

(U//~~FOUO~~) NSA is concerned about privacy and anonymity not only in an organizational context, but is also sensitive to the exposure of its employees as individuals in this regard. Agency employees are subject to the same threats to their privacy as other members of society. Whether it is a case of careless use of wireless equipment or unauthorized dissemination of biometric data, individuals working for NSA are at risk for invasions of their privacy, a contingency that can lead to the Agency also being harmed.

(U) Introduction

(U) This paper is not intended to be a conventional technology forecast. For one thing, privacy and anonymity are not technologies, as are the subjects of most previous forecasts. Rather they are abstractions which over time have become enshrined in democratic societies as basic rights. Since the dawn of the Internet age, the status of these rights has been viewed by civil libertarians as more threatened, but just as inalienable, as before. In the period after 9/11, however, there is strong support from other quarters for tempering privacy guarantees in the interest of security. Developments related to these issues in the United States and elsewhere will be one focus of this paper.

(U) The paper will also contain information on certain technologies which either are designed to protect the privacy and/or anonymity of computer users, or which have other privacy implications, but it will not provide an in-depth examination of any single technology. In fact, a few of the technologies briefly discussed here have already been the subject of--or covered to some degree by--earlier more comprehensive forecasts, including PKI (Public Key Infrastructure), Wireless, IDS (Intrusion Detection Systems), VPN (Virtual Private Networks) and Biometrics. Nor will it be a comprehensive treatment in the sense that every privacy-protective technology and tool will be discussed. (A lengthy list provided by the Electronic Privacy Information Center is found in Appendix I.) Instead, the focus will be on a few of the technologies singled out by Government customers as of special interest, and the way in which privacy and anonymity concerns are pushing technology.

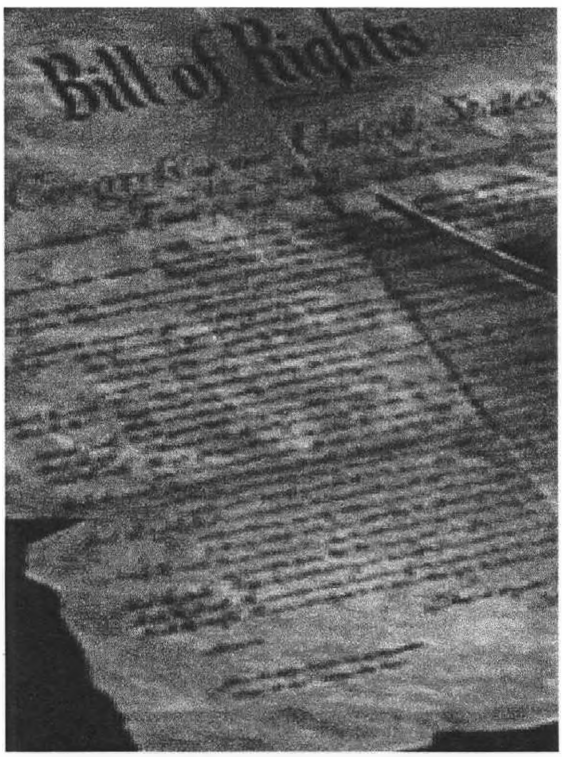
(U) The U.S. public, and indeed people the world over, are increasingly concerned about their online privacy. In democratic nations, legislators have passed laws to protect their constituents in this regard. Some of the legislative highlights, most notably in the United States and European Union, will be covered in this paper. Although many observers consider statutory solutions more effective than technological means, in some societies the government is the biggest threat to privacy and is not inclined to take action to protect its citizenry. Even in those cases where governments are favorably disposed to the privacy rights of their people and where protective laws have been passed, those laws are often deemed insufficient by civil libertarians. Hence, technological answers to the problem have also been sought and will continue to be. Some of these technologies which have emerged over the years to address the challenge, and flaws in those technologies, will also be discussed in this forecast. What is clear is that, regardless of a government's good will and benign conduct, security and privacy are inextricably interwoven. If security is not built into the application of a technology, threats to privacy will appear from some quarter or the other.

(U) As the title indicates, this is a paper on both privacy and anonymity. Though there is a relationship, they are by no means the same thing. For purposes of this paper, "privacy" will be used to denote the right of individuals and organizations to control their online personal or proprietary information. Furthermore, this right, while not absolute, is limited only to the extent that the needs of society as a whole require that the information be shared. Otherwise, individuals and other owners should be able to decide those to whom they will communicate their personal information--perhaps, for example, as a condition for receipt of services or goods. "Anonymity", on the other hand, will be used to refer to the right to conceal one's identity when active online.

Though sometimes an end in itself, it is also one means of maintaining personal privacy. Some would go so far as to say anonymity, especially where there is an oppressive government, is a *sine qua non* for privacy.

(U//~~FOUO~~) These concepts have obvious implications for NSA, both in connection with its SIGINT and Information Assurance mission. Because of classification considerations, this paper will not consider privacy and anonymity ramifications for the Agency in any depth. What can be said, however, is that as technology enhancements occur in response to threats to online privacy and anonymity, the Agency's performance of its intelligence mission will likely be more challenging and expensive, while its Information Assurance mission can be either assisted, or made more difficult.

(U) Background



(U) Privacy and anonymity did not first surface as an issue or right with the advent of Information Technology (IT). For example, James Madison and Alexander Hamilton, both authors of the U.S. Constitution, made their contributions to *The Federalist Papers* anonymously, thereby witnessing to their position on the matter. Over the past 200 years, Americans have come to view privacy as sacred as some of the other rights found in the Constitution, and when they perceived their privacy being threatened, they have vigorously resisted the invasion. Some argue that the Founding Fathers saw privacy as a natural right, indispensable to life, liberty, and the pursuit of happiness. Not even the most outspoken of privacy advocates, however, claims that the right to privacy is absolute, or that it is explicitly enshrined in the Constitution, for it is not. Nevertheless, jurists do believe that it is present implicitly in at least both the Fourth and Fifth Amendments.[1]

(U) Dramatic advances in technology during the late 20th Century through the infancy years of the 21st have magnified concerns about threats to this cherished right. Some of these technologies were developed to respond to the legitimate requirements of business and government for easier access to information about individuals, but have in effect made it a challenge for computer users to preserve their privacy.[2] All three branches of our Government have acted in response to these concerns, at times having to weigh in the balance the countervailing merits of other claims by the public welfare. For example, the Federal Trade Commission has expanded its role in the area of information privacy over the past seven years,[3] although the United States does not have a true privacy oversight organization akin to that of the European nations and other countries. The U.S. Courts have also been active over the years, with the Supreme Court ruling that a number of Constitutional Amendments protect privacy.[4] While not directly related to IT, a June 2002 decision of the Supreme Court held that door-to-door canvassers have a right to anonymity when expressing their religious beliefs. As for the Congress, few social issues have been the subject of as much legislative activity in recent years as that of privacy. The Financial Services Moderniza-

1. (U) "Privacy and Security on your PC," *Extreme Tech*, 28 May 2002.
2. (U) "Guide to Online Privacy," Chapter Three: Existing Privacy Protections," *Center for Democracy and Technology*, 1998-2000.
3. (U) "Hearing on the Reauthorization of the Federal Trade Commission," *Center for Democracy and Technology*, 17 July 2002.
4. (U) Walton, Timothy J. "Internet Attorney," *Internet Privacy Law*, 2000.

tion Act of 1996 (Gramm-Leach-Bliley Act), the Health Insurance Portability and Accounting Act (HIPAA) of 1999, the USA PATRIOT Act of 2001, and legislation introduced in 2002 to study the proper balance between privacy and security are just four examples of Congress asserting itself on this issue.

(U) U.S. Legislation

(U) Although Gramm-Leach-Bliley concerns matters other than privacy, it does contain provisions intended to provide a degree of customer protection with regard to personal financial data. Privacy advocates argue that the statute does not go far enough. For instance, the law gives consumers only an "opt-out" choice, which means that they must actually notify a company that they do not want their data shared. Another requirement of the law is that a company must notify consumers of its privacy policy, i.e., what data it collects, how it uses and with whom it shares the information. Privacy policies, however, can be altered "overnight," without a customer being aware at the time.[5]

(U) For most people, the records likely considered most sensitive are those concerned with their health. Reflecting widespread public anxiety in this regard, in 1996 Congress passed HIPAA which called on the Department of Health and Human Services (HHS) to develop regulations for the protection of privacy of personal health data, if Congress itself had not set standards by August 1999. When Congress did not meet this deadline, HHS-issued regulations went into effect in April 2001, with health organizations having until April 2003 to achieve full compliance. These regulations embody certain basic principles which include: consumer control of information, data use for health care purposes only, criminal sanctions for misuse or improper disclosure of personal health information, and need to balance privacy and public health needs.[6]

(U) Less than 2 months after 9/11, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, usually referred to as the USA PATRIOT Act. Loaded with enhanced surveillance powers for the Government, the law also sets limits on how far authorities can go to prevent terrorism. Nevertheless, there is no question that the scale tips in favor of giving the Government the power it wants to thwart future acts of terrorism. Civil libertarians cite a number of provisions which they find troublesome, including Section 216, which mandates "tracking" of certain telephone and Internet information. Privacy advocates consider the Act's distinction between "dialing, routing, addressing, and signaling information" on the one hand, and "content" on the other, as unclear, since email messages consist of packets wherein the two categories are mixed. Section 216 prohibits tracking of only the latter. Apart from privacy concerns, Internet Service Providers are expressing concern about the costs of responding to a significantly higher number of requests for information from law enforcement authorities, since the Act's passage.

---

5. (U) Givens, Beth. "Eight Reasons to be Skeptical of a 'Technology Fix' for Protecting Privacy." *Privacy Rights Clearinghouse*, 14 October 2000.
6. (U) Ledford, Jerri. "Ensuring Privacy and Security for Medical Systems." *Faulkner Information Systems*, February 2002.

(U) Partly as a reaction to the significant increase in governmental surveillance powers and associated emerging technologies which are being developed to exercise that authority, Senators Charles Schumer and John Edwards pushed a bill in the summer of 2002 to set up a commission to study the proper balance between privacy and security. The senators' proposed legislation (not passed as of the date of this paper) calls for an examination of technologies with the potential to threaten privacy.

(U) International Privacy Protection

(U) In those countries around the world where privacy concerns appeared ascendant before 11 September 2001, that dominance has been tempered somewhat over the past year. The Parliament of the European Union (EU) in May 2002 passed the Communications Data Protection Directive over the strong objections of civil libertarians. By a substantial majority of 351 to 133, Parliament passed the measure on the basis that for anti-terrorism purposes, the authorities must be able to view customer data related to their email, fax, Internet and other transmissions. Under the legislation, telecommunication companies must, if directed, retain specific customer transmission data for an indefinite period. At the same time, there are significant provisions in the directive safeguarding citizens' privacy. For example, there will be an "opt-in" policy on unsolicited commercial e-mail or spam. Also, mobile users must approve use of privacy sensitive location data, and they will be able to block temporarily the processing of location data.[7]

(U) In October 2001, President Bush had asked the European Union to revise the directive, so as to allow retention of telecommunications data for longer than the 1- or 2- month period required for billing purposes, as called for in the draft. The directive--which in its final form approved by the Parliament allows retention for an indefinite period-- must now be approved by the 15 member states. The outcome is uncertain, because of cost concerns, as well as continuing objections on the part of civil libertarians who remain active throughout the EU. In a June 2002 manifestation of this strength, the British Government set aside a proposal to extend police access to telephone and Internet data, after privacy activists demurred. In addition, even already existing UK national security legislation is being challenged on human rights and privacy grounds.

(U) Many in U.S. business and government circles in recent years had been unhappy with aspects of the EU privacy approach, which entails establishment of data protection agencies, and registration of data bases. [8] On the other hand, Europe's 1990's Privacy Directives are considered by many here and abroad as a model for the rest of the world to copy, but their impact on U.S. commercial interests has been troublesome, especially as the regulations relate to multinational corporations conducting trans-Atlantic business. To ensure adherence to the EU regulations, the U.S. Commerce Department drew up a Safe Harbor arrangement to work in conjunction with EU directives.[9] This framework has made it possible for U.S. companies to continue doing business with the EU while avoiding regulatory pitfalls in the privacy arena. Nevertheless, in a sign of con-

7. (U) "Proposal for a Directive of the European Parliament," Commission of the EC, 30 May 2002.
8. (U) "Welcome to the Safe Harbor," U.S. Department of Commerce, 2000.
9. (U) Carey, Alan. "Worldwide Information Security Services Forecast, 2001-2006," *IDC Report #26899*, April 2002.

tinuing unhappiness with EU rules, a group of 10 U.S. companies which calls itself the Global Privacy Alliance, in the fall of 2002 was pressing the European Commission to change its regulations with respect to transnational data flow.

(U) Besides Europe, other regions and nations are also wrestling with privacy issues in varying degrees. Canadian legislation, which became effective in 2001, places the burden of ensuring privacy mostly on business, but consumers are responsible for bringing complaints to the Canadian Privacy Commission that has the power to fine firms up to $100,000 for violations.[10] In Asia, there is also a growing concern about privacy protection. For example, in August 2002 Japan initiated a computerized national ID system involving an 11-digit identification number which encountered vigorous opposition because of privacy concerns. Although no significant privacy laws have been passed to date in Latin America, Brazil and Mexico have bills pending regarding digital signatures and e-commerce.[11]

(U) U.S. Government Privacy Concerns

(U) The concept of privacy is ordinarily thought of in terms of the individual person. Organizations, however, also have privacy needs. Infringements of corporate privacy may not be felt as personally, but they can be nevertheless damaging.[12] Even governments, often thought of more as a threat to individual privacy, have a need for it. U.S. Government agencies are subject to invasions of privacy, and there have been numerous documented successful intrusions into or attempts against public systems which have resulted in a loss of privacy, or which have had the potential for this outcome.

(U) During 2002 alone, there have been reports of computer and network security lapses at the Defense Information Systems Agency (DISA), National Aeronautics and Space Administration, Veterans Administration, and Drug Enforcement Administration (DEA). Although the DEA incident entailed criminal activity on the part of an insider, privacy advocates were quick to call attention to the danger stemming from the multiplicity of law enforcement data bases which "hundreds of thousands" of people can access.[13] With reference to DISA's problems, one outside expert explained the lapse on the basis that "This could happen to anyone, because people are deploying systems before thinking about security."[14] The National Institute of Standards and Technology (NIST) was doubtless aware of the DISA situation when it issued its draft report on Wireless Network Security in July 2002, urging federal agencies to exercise caution in deploying wireless Local-Area Networks (LANs).[15]

10.(U) Greene, Joe and Gaw, Jonathon. "Security and Privacy: Inextricably Linked." *IDC Bulletin #CA0751EJ*, April 2002.

11. (U) Carey, Alan. "Worldwide Information Security Services Forecast, 2001-2006," *IDC Report #26899*, April 2002.

12. (U) Wheatman, Vic. "Corporate Privacy," *Gartner Letter from the Editor*, 23 October 2001.

13. (U) Poulsen, Kevin. "DEA Data Thief Pleads Guilty," *Security Focus Online*, 7 August 2002.

14. (U) Brewin, Bob and Verton, Dan. "DoD IT Projects Come Under Fire," *Computerworld*, 16 May 2002.

15. (U) Karygiannis, Tom and Owens, Les. "Draft, Wireless Network Security, 802.11, Bluetooth and Handheld Devices." *NIST Special Publication 800-48*, 29 July 2002.

(U) In the year since the 9/11 attacks, numerous warnings have been issued about the threat to the U.S. IT infrastructure, including that portion of it owned by the Government itself. U.S. Government agencies--sometimes lackadaisical in the past--have taken the threat to heart, awarding new contracts to cybersecurity firms and in the case of the Defense Department, taking steps to prohibit certain high-risk devices (most wireless equipment) from being used at DoD installations. It remains to be seen if this heightened awareness and resolve will survive the present period of post-9/11 anxiety, or will fade somewhat in the absence of further catastrophic terrorist attacks. In any event, concern about the security and privacy of wireless LANs, as well as of other IT technologies, will drive both public and private sector users to push for solutions.

(U) Technology Evolution

(U) Since the dawn of the Information Age, engineers have been seeking solutions to the inevitable vulnerabilities that appear as quickly as new technologies enhancing the utility and performance of computers. As the Internet came of age and computer use mushroomed, users and non-users alike became increasingly concerned about exploitation of security weaknesses and what they viewed as inadequate protection for personal information. The faster and more powerful the systems became, the greater the potential for both good and mischief. Likewise, the greater the volume of personal information entering data bases, the stronger was the urge to benefit--for ethical or unethical purposes--from access to and use of the information. Concern about this gave rise to a number of technologies designed to provide the security needed for the preservation of data privacy. Some of these technologies are discussed below, as well as certain technologies that have been the driving force for the emergence of some of these defenses. Anonymity will be highlighted since, like some of the technologies mentioned here, it is viewed by many as one of the most important tools for providing privacy. Although not a technology itself, it has spawned a multiplicity of protocols with varying degrees of effectiveness.

(U) Anonymity

(U//~~FOUO~~) As suggested in the Introduction, anonymity is not synonymous with privacy. Since the earliest days of the Internet, however, anonymity has been widely considered a crucial contributor to acquisition and maintenance of the privacy which most computer users desire. Therefore, it needs to be discussed in this paper. As for NSA, it has deemed anonymity as an end in itself, for without it, the Agency would not be able to carry out certain essential facets of its mission. (See **NSA Related Activities** Section.)

(U) In a case not involving computer use, the right of a U.S. citizen to remain anonymous when expressing religious or political views has been upheld by the Supreme Court, most recently in the summer of 2002,[16] suggesting such activity online is likely constitutional. Individuals seeking anonymity online--whatever the subject and wherever they are--may do so for either proper or improper ends. They could be terrorists, or they could be law-abiding citizens who simply desire to keep their identity a secret for a totally legitimate reason. In other societies which lack basic freedoms, they may want to express views which are repugnant to their own government, but acceptable in free societies. Whatever the purpose of the user, computer services and numerous protocols exist to accommodate both the terrorist and the legitimate user. While they may not provide absolute anonymity, the effectiveness of some for purposes of the average person is generally adequate, though not riskfree.[17] In fact, few-- if any-- are totally successful. Even the respected SafeWeb anonymous-surfing technology was found to have flaws that permitted concealed Internet addresses of a visitor and addresses of sites visited to be revealed through use of

16. (U) U.S. Supreme Court, Watchtower Bible & Tract Society v. Village of Stratton, 17 June 2002.
17. (U) Wright, Matthew and Adler, Micah et al. "An Analysis of the Degradation of Anonymous Protocols." *Proceedings of the ISOC' Network and Distributed System Security Symposium (NDSS 2002)*, February 2002.

Java- Script. Meanwhile, as even newer technologies emerge, some of them (see Palladium below) are seen as threats to the limited anonymity which is available, for example, through P2P (Peer-to-Peer) computing.

(U) Remailers, which are designed to hide the origin of an email message, are one such service. (See Appendix I.) There are two general categories: pseudo-anonymous and truly anonymous. The pseudo- anonymous remailers are those that strip off the header information, but whose operators still know the email address of the user. In the case of the truly anonymous remailer (Cypherpunk and Mixmaster), the operator does not know the user's identity. Remailer operators who send email through the Mixmaster system claim that all identifying data will be removed from the header, that the message will be encrypted, and that it will pass through several Mixmaster remailers before arriving at the computer of the intended recipient. Not surprisingly, this circuitous route usually entails a lengthier voyage for the email, typically half a day. Experts recommend that anonymous mailers have 128-bit SSL (Secure Socket Layer--see below) encryption on their browsers, and also an HTTPS connection with SSL encryption. Another suggestion of some security experts is that the connection with the remailer should be through a web proxy.

(U) Web proxies, used by anonymizers, are also helpful for hiding a surfer's IP address and for disabling cookies, messages sent by Web servers to a browser to keep track of user activity. Anonymizing services (i.e., anonymizers) prevent Web sites from gathering information from visitors, even concerning what sites they visit. By using a proxy, ideally only the IP address of the proxy is visible to a visited web site, so a user appears to be originating from the proxy. In reality, many proxy servers transfer client IP information, although not in the standard form. SOCKS-protocol proxies, because they are non-caching, are held to be the best general-purpose proxies and succeed in hiding client IP addresses. Anonymity layers established with the most effective protocols can be further strengthened by selecting a proxy server in another country, especially one where the user's language is rarely spoken or where officials are unlikely to respond positively to a foreign request for logs.[18] A number of other techniques are available to the average user for enhancing online anonymity, but none to date has proven absolutely foolproof.

(U) In the summer of 2002, a new P2P protocol was to be unveiled by the hacker organization Hacktivismo which purportedly will significantly upgrade anonymity capabilities. Called "Six/Four" (named after the June 4, 1989 Tienanmen Square massacre), the protocol will reportedly use the referenced P2P technology, along with virtual private networking and web proxies, to achieve enhanced anonymity.[19] As of the time of this study, peer review results assessing the new protocol were not available to the author of this study.

(U) Among others in the academic world, a Georgetown University researcher is working to improve anonymity for the Internet user. Clay Shields, a co-author of the anonymity protocol degradation study cited above, is attempting to develop "a network in which users are guaranteed anonymity unless they misbehave, at which point they will be able to be identified and held accountable for their actions only by legitimate authorities."[20]

---

18. (U) Greene, Thomas C. "Do-it-yourself Internet Anonymity," *The Register*, 1 July 2002.
19. (U) Harrison, Ann. "Peer-to-Peer Anonymization," *Network World Peer-to-Peer Newsletter*, 24 July 2002.
20. (U) Shields, Clay. "Statement of Research Interests," Georgetown University, 2002.

(U) PKI

(U) PKI (Public Key Infrastructure) uses a widely disseminated public key, while the user has sole knowledge of his secret or private key. The infrastructure offers two basic services: 1) certification achieved through certificates issued by a trusted certification authority (CA) and 2) validation, which provides verification of a certification's ongoing authenticity.[21] Through the use of a digital signature, PKI also provides assurance of data integrity, i.e., non-alteration of the data after it leaves the sender. In addition, non-repudiation is made possible by a digital signature, which is designed to make it difficult for a sender to deny signing or originating a document or transaction.

(U) In the mid-90s, the U.S. Government promoted the Clipper chip which contained a strong encryption algorithm, but the technology was seen as a privacy threat because of its escrow feature. As a general rule, however, robust cryptography has been considered a major bulwark for protection of privacy. For example, Public Key Cryptography, which came into use in the mid-1970s for provision of essential security services, is considered by many as an invaluable asset in the struggle for protection of privacy. It is heavily dependent on a functioning PKI for its success. No longer primarily an "end product," PKI is increasingly being integrated into applications. SSL and IP security-based Virtual Private Networks (VIPs) are two examples of this phenomenon of PKI integration.[22]

(U) Cost and complexity, as well as other factors, have contributed to a slower enterprise adoption of the technology than was anticipated a few years ago. The value of PKI is proportional to the number of users who have it. Over the next few years, only a small minority of business-to-business (B2B) and business-to-consumer (B2C) transactions will have the benefit of crypto-based digital signatures, meaning repudiation will remain a possibility. As a result, businesses have been cautioned to be wary about heavy investments in digital signatures.[23] Some observers believe that PKI vendors need e-commerce more than e-commerce needs PKI.[24]

(U//~~FOUO~~) NSA, with responsibility since 1999 for oversight of the Defense Department's PKI use, has been encouraging its own personnel to obtain PKI certificates, if they do not already have them. The Agency is confident that the certificates will provide both confidentiality and data integrity, as well as prevent unauthorized access and spoofing. PKI is viewed as only one component, though an important one, of its comprehensive Defense-in Depth program.

---

21. (U~~FOUO~~) Cameron, William L. "Public Key Infrastructure. A Technology Forecast," Office of INFOSEC Research and Technology, August 1999.
22. (U) Wheatman, Vic. "Public Key Infrastructure 1 H02 Magic Quadrant." *Gartner Research Note*, 14 February 2002.
23. (U) Wheatman, Vic. "Questioning the Value of Digital Signatures," *Gartner Commentary*, 17 June 2002
24. (U) Ellison, Carl and Schneier, Bruce. "Ten Risks of PKI: What You're Not Being Told about Public Key Infrastructure." *Computer Security Journal, Volume XVI, Number 1*, 2000.

(U) SSL (Secure Socket Layer)

(U) Netscape-developed SSL, a protocol which uses a public key for encryption of data transmitted over the Internet, is considered mainstream today. Through SSL, or the Internet Engineering Task Force (IETF) next-generation Transport Layer Security protocol, consumers usually feel confident of the authenticity of the retail or banking service they are dealing with. When the characteristic yellow lock or blue key appears on their screen, they believe their credit card number or other personal information entrusted to an Internet link will remain private. Gartner also attributes SSL's achieving a mainstream status since its appearance in 1994 to the fact that CAs make it a requirement that 1) the domain name really belongs to the business applying for a public-key certificate and 2) the name appearing on the certificate really is that of the applicant.[25]

(U) Despite continuing widespread confidence in the SSL technology and in its ability to provide privacy, flaws do exist. Some experts consider SSL authentication weak, and expect that there will be movement towards employment of XML (Extensible Markup Language) technology for securing transactions. Researchers have found SSL problems which one called "severe." According to a report by one such researcher, Mike Benham, Internet Explorer is subject to "man-in-the-middle-attacks" which would allow "anyone with a valid CA-signed certificate for ANY domain" to create "a valid certificate for ANY OTHER domain (capitals in original)."[26] Others are also concerned that low-cost certificates and shortcuts in acquiring them will result in SSL becoming an "ineffective security facade."[27] In another report critical of SSL technology, researchers at Netcraft, a British firm, have found that hackers can break a server's public key if it is shorter than 1,024 bits. They can then "impersonate" the server. The problem is more severe in Europe than in the United States, since key length is not evident to most users who may not even be aware they are still using the 512-bit key, the previous upper limit dictated by former U.S. export restrictions on strong cryptography.[28]

(U) Digital Rights Management and Privacy

(U) Unlike PKI and SSL, Digital Rights Management (DRM) technologies are not designed primarily to provide privacy-enhancing qualities, but they do raise privacy issues which should be mentioned in this paper. Most observers agree on their purpose as being mainly protection for copyright holders. Nevertheless, supporters also assert that some of these technologies, notably Palladium, offer a degree of privacy protection, as well as a defense against viruses and maybe even spam.

---

25. (U) Pescatore, John and Wheatman, Vic. "Secure Sockets Layer Sometimes Isn't," *Gartner Research Note*, 3 April 2002.
26. (U) Edwards, Mark Joseph. "Severe Vulnerability in Internet Explorer SSL," *Wininfo InstantDoc #26245*, 13 August 2002.
27. (U) Pescatore, John and Wheatman, Vic. "Secure Sockets Layer Sometimes Isn't," *Gartner Research Note*, 3 April 2002.
28. (U) Rohde, Laure. "Study: SSL Encryption Weaker in Europe than in U.S.," *IDG News Service*, 3 April 2002.

(U) P2P protocols, mentioned in the earlier section on Anonymity, made possible widespread anonymous swapping of music and even video files, which became a major source of consternation for the recording and movie industries. For example, several hundred thousand movies are estimated to be downloaded illegally over the Internet each day. [29] Because of the entertainment industry's and others' concerns, the Digital Millennium Copyright Act was passed by Congress in 1998 to criminalize the development and use of DRM circumvention tools. Other legislation is currently being considered by Congress to strengthen the position of copyright holders. Sensing Congressional support, the Motion Picture Association of America and AOL Time Warner have been tracking down digital pirates and interfering with illegal downloading, and in some instances, having their Internet service cut off. The music industry has also gone on the offensive by substituting bogus files, such as recordings which repeat a single verse numerous times.

(U) Microsoft and others have tried to help out copyright holders by developing DRM technologies, but these have often been seen by civil libertarians as invasive of privacy rights. In essence, DRM is intended to help content owners control use and distribution of their files, privacy advocates contend. They argue that a requirement for identity disclosure and information on a user's rights to the content, before access to the content is granted, constitutes a violation of privacy. [30]

(U) In June 2002, Microsoft announced its Palladium initiative which is its planned implementation of the Trusted Computing Platform Alliance architecture. (The alliance is a group of about 180 companies, including IBM and Microsoft, which committed itself to producing an industry specification for improvement of authenticity, privacy, and trustworthiness on the Internet.) The following month, some details were revealed, which immediately increased already existing privacy concerns on the part of civil libertarians, despite the claim by Microsoft that greater, not reduced, personal privacy features are being designed into the technology.

(U) Critics demur, retorting that privacy will be diminished inasmuch as every typed character can be traced back to the user. In a blow at anonymity, the technology will reportedly make it possible for originators and recipients of email, for example, to be identified without great difficulty. What makes this possible are hardware and software features which will be part of a package facilitating control of copyright material by holders. Detractors claim that placement of hardware encryption keys on the computer motherboard lies at the heart of the system, thereby enabling identification of that motherboard by any software application. It was Microsoft DRM research that led to the development of this encryption technology. In a possible attempt to downplay its DRM application, Microsoft has described Palladium, which will probably be released no earlier than 2004, as only a "stepping stone" to DRM. [31]

(U) Some observers, however, fear that the stone can be turned into a weapon. They point to Microsoft's earlier (introduced in 1999) Passport System--with some features similar to Palla-

---

29. (U) "Consumer Benefits of Today's Digital Rights Management (DRM) Solutions: Hearings before the Subcommittee on Courts, the Internet, and Intellectual Property of the Committee on the Judiciary, House of Representatives, 107th Congress, Second Session, 5 June 2002, Serial No.72."
30. (U) "Digital Rights Management and Privacy," *Electronic Privacy Information Center*, 11 July 2002.
31. (U) Kearns, Dave. "I'm from Microsoft, and I'm Here to Help You," *Network World*, 15 July 2002.

dium--as well as the Liberty Alliance's specification announced in July 2002, as examples of products advertised as upgrading security and privacy, but not always fulfilling their promise. These identity services, offering SSO (Single Sign-On) and digital wallet features, are a threat to anonymity on the Internet, since users' online activities can be tracked, according to privacy advocates. But not all researchers agree that this dire outcome is a foregone conclusion. Some say that as long as individuals can use "cyberaliases" to hide their true identities, privacy and anonymity will survive Passport and the Liberty Alliance.[32] Nevertheless, Passport did not stand up to the scrutiny of the Federal Trade Commission, which forced Microsoft in August 2002 to back off from exaggerated assertions about security and privacy features afforded by Passport.

(U) As with Passport and the Liberty Alliance specification, Palladium and similar technologies will also have to be examined closely with respect to their privacy and other (e.g., antitrust) implications. Forrester research analyst Laura Koetzle has perhaps raised the ultimately most pertinent question, even more so than the privacy issue. Will users activate Palladium, which will be offered on an opt-in basis? "What's in it for consumers?" she asks. It remains to be seen whether Microsoft's claims of enhanced system security will be persuasive to computer shoppers, or whether they will agree with Koetzle who maintains that the technology makes sense for the computer industry and other copyright holders, but probably not for the average user.[33]

(U) Virtual Private Network

(U) A Virtual Private Network (VPN), attractive to many enterprises because of clear cost savings offered, uses the public telecommunication infrastructure for the creation of a private data network. The automotive is just one example of an industry which has eschewed leased lines in favor of VPNs for their extranets.

(U//~~FOUO~~) IPsec, short for IP Security and developed by the IETF, has been widely used for secure packet exchanges on VPNs. One high performing IP processor is the BCM5841, announced by Broadcom in September 2002. It features Advanced Encryption Standard (AES) support with 256-bit key processing. A VPN provides data encryption in advance of the data's transmission through the public network, and decryption when it reaches the intended recipient. Privacy is achieved through a tunnelling protocol which encrypts both the data and the header. Less secure than the tunnel mode is the transport mode which encrypts only the data portion, also known as the payload.

(U) Over the past year or so, some businesses are looking into multiprotocol label switching (MPLS) for their VPNs. Instead of IPsec encrypted tunnels, VPNs using MPLS services create "label-switched paths," which can pose security risks and even leave a VPN open to a denial-of-service attack. On the other hand, IPsec VPNs do not necessarily afford significantly more security and privacy than MPLS VPNs, since the Internet-connected end points of an IPsec VPN are open to attack. According to at least one expert, when an MPLS user has concern about the security of its Internet-shared backbone, the firm should consider purchasing an IPsec overlay network

32. (U) Pescatore, John. "Identity Services Do Not End Privacy Online." *Gartner Commentary*, 29 March 2002.

33. (U) Costal, Sam. "Microsoft Offers Palladium Details." *IDG News Service*, 29 July 2002.

for encryption of its MPLS data. [34]

(U) Notwithstanding the security concerns expressed by some researchers about SSL which were cited earlier in this paper, SSL is regarded as cheaper and more secure than an IPsec solution, depending on the applications an enterprise wants to carry over a VPN. For remote access and extranet purposes, SSL VPNs, which use a combination of SSL encryption and proxies, are gaining acceptance as a preferred solution. If limited to browser or HTTP-based applications, Gartner suggests that SSL is cheaper and more secure than traditional IPsec. [35]

(U) As their name suggests, VPNs are really designed to provide privacy more than security. Their main function is to serve as a mechanism furnishing privacy between two points. Gartner considers cost savings or unavailability of legacy private networking services as good reasons for choosing a VPN, but security improvement is a "wrong reason" to implement a VPN, it maintains.[36] Therefore, security must be achieved through an enterprise integrating other technologies, such as PKI. In response to this perceived need, in March 2002 a new PKI-enabled wireless VPN was announced by Columbitech AB and Diversitech (see under **Wireless** Section which follows).

(U) Wireless Technology

(U) The term "wireless" generally is used to refer to 802.11 and 802.11b technology for Wireless Local Area Networks (WLANs), as well as frequency bands used for General Packet Radio Service, 2.5G, and the emerging 3G technologies. Concern about the security and privacy of the technology only seems to increase as time passes. In one of the more publicized instances of demonstrated wireless security inadequacy on the part of a Government agency, the Defense Information Systems Agency's (DISA) WLAN on 10 May 2002 was detected and scanned in under half an hour by a contractor. In July 2002, NIST issued a draft report about the serious vulnerabilities of wireless networks and advised U.S. Government agencies to be exceedingly cautious about implementing them. [37] In September, President Bush's Critical Infrastructure Board followed in the same vein, with the release of its National Strategy to Secure Cyberspace.

(U) The Institute for Electrical and Electronics Engineers (IEEE) developed what is probably the best known wireless standard, IEEE 802.11b (Wi-Fi), but it has been widely criticized for its shortcomings. Security flaws in the 802.11b's cipher key scheduling algorithm and in IEEE's associated WEP (Wired Equivalency Privacy) protocol, have been well documented. Analysis done in 2001 by University of California researchers resulted in a recommendation that users of 802.11 networks not count on WEP for security. The warning applied to both the 40-bit and the 128-bit WEP versions.[38] Another 2001 study, done by researchers from Israel's Weizmann Insti-

34. (U) Rickard, Neil. "Do MPLS VPNs Deserve to be Called Private?," *Gartner Research Note*, 5 March 2002.
35. (U) Pescatore, John and Wheatman, Vic. "Management Update: Gartner's Information Security Hype Cycle Helps to Cut Risks," *InSide Gartner*,28 November 2001.
36. (U) Girard, John and Pultz, Jay. "The Pros and Cons of Building a VPN," *Gartner Research Note QA-14-1811*, 30 August 2001.
37. (U) Karygiannis, Tom and Owens, Les. "Draft, Wireless Network Security, 802.11, Bluetooth and Handheld Devices." *NIST Special Publication 800-48*, 29 July 2002.

tute of Science and Cisco Systems, described a theoretical method of attack against WEP.[39] Less than a week later, researchers from Rice University and AT&T labs, using the information from the latter report, were able to implement a successful attack against the WEP encryption protocol and to recover the 128-bit secret key.[40]

(U) Another WEP iteration, known as 802.1x and reportedly to be released in late 2002, changes encryption every few minutes and attempts to address WEP authentication problems, but it too is considered vulnerable. Given WEP's weaknesses, VPN installation is regarded by many experts as the answer with the greatest potential for filling the gaps inherent inWLAN technology.

(U) In addition to the issues raised in the wireless arena by the inadequacy of the WEP, privacy advocates are also troubled by threats posed to wireless users by the increasingly accurate capability of providers to locate users of wireless phones and PDAs. Privacy groups have urged the Federal Communications Commission to set rules which would protect wireless location information. Although locational technology, like others, has the potential to yield many benefits to society, civil libertarians are concerned that it can also be used in an irresponsible fashion to invade the privacy of law-abiding citizens.[41]

(U) Platform for Privacy Preferences

(U) On 16 April 2002, the World Wide Web Consortium (W3C) issued the Platform for Privacy Preferences Project (P3P), which is designed to allow visitors to websites greater control over their personal information. W3C, the Web's main standards organization, wants to provide users a means of specifying the amount of data collection and sharing they are willing to permit, and a means of verifying that the limits have not been passed. This is accomplished by software which reads websites' privacy policies. When there is not a match with a user's stated requirements, the software advises the visitor to the site. Although P3P makes it possible for a user to be aware of a website's stated privacy practices without having to read through these often lengthy statements, the W3C concedes that there is no guarantee that a site will abide by its own policy.[42]

(U) The W3C came into existence for the purpose of developing common protocols which would contribute to the Web's interoperability and growth. Development of P3P began in the mid-90's when members of W3C working groups and the Center for Democracy and Technology (CDT) agreed to work on getting industry support for responsible use of private information by websites. Ultimately, international leaders in not only industry, but also government and academia, collaborated in the creation of P3P. A P3P demonstration privacy tool was unveiled at a 1997 Federal Trade Commission privacy workshop, and by 2001 about 100 companies and orga-

38. (U) Borisov, Nikita et al. "Security of the WEP Algorithm," *University of California Paper*, July 2001.
39. (U) Mantin, Istil et al. "Weakness in the Key Scheduling Algorithm for RC4," Paper Presented at Toronto Cryptographic Conference, August 2001.
40. (U) Stubblefield, Adam. "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP," *AT&T Labs Technical Report TD-4ZCPZZ, Revision 2*, 21 August 2001.
41. (U) "Wireless Location," *Center for Democracy and Technology*, 30 July 2001.
42. (U) Cranor, Lorrie and Langheinrich, Marc, et al. "The Platform for Privacy Preferences 1.0 (P3P1.0 Specification)," W3C, 16 April 2002.

nizations had implemented P3P on their sites. In the same year, Microsoft included P3P on Internet Explorer (IE).[43]

(U) Intrusion Detection Systems

(U) An Intrusion Detection System (IDS) has been likened to an alarm system. As a burglar alarm warns of an intrusion into a home or other personal place, an IDS detects illicit access or even access attempts into a computer system. Although not all computer intrusions represent an effort to obtain personal information from the system, such attacks need to be considered as a potential threat to sensitive data of a private nature residing on many systems.

(U) Intrusion Detection Systems had their origins in the audit systems of the 1950s.[44] An IDS works by examining or auditing network activity and identifying specific suspicious events. Unlike a firewall, which is designed to prevent an intrusion, an IDS monitors events which are already underway.

(U) One of the main categories of IDS systems, the network-based system (NIDS which expands to Network Intrusion Detection System), analyzes packets already moving through the network. One such NIDS is SNORT, which provides "real-time traffic analysis and packet logging on Internet protocol networks."[45] A host-based system, by contrast, monitors system logs for signs of malicious activity. This latter IDS category is viewed by many as inferior in several respects. Host-based systems are more costly and miss attacks which NIDs detect. Also, NIDs detect an attack while it is underway, while a host-based system's strength lies in the assistance it provides in discovering and understanding past attacks.

(U) Biometrics

(U) Of the many technologies with privacy implications, perhaps none is fraught with more drawbacks in the opinion of privacy advocates than biometrics. While identification techniques using people's physical features offer tempting possibilities for improving security and preventing fraud, the privacy ramifications continue to be troublesome for many Americans who are fearful that an intrusive "Big Brother" might misuse stored personal profiles. In addition, there is anxiety about the threat of identity theft resulting from profiles being acquired by unscrupulous individuals. Since 9/11 these concerns have not been muted by the argument that increased security can be achieved only if certain concessions are granted to the Government.

(U) Biometrics are defined as "the automated use of physiological or behavioral characteristics to determine or verify identity."[46] The most promising technologies to date involve scanning

43. (U) Cranor, Lorrie Faith. "The Role of Privacy Advocates and Data Protection Authorities in the Design and Deployment of the Platform for Privacy Preferences." Remarks at the Twelfth Conference on Computers, Freedom and Privacy, San Francisco, April 16-19,2002

44. (U/~~FOUO~~) Lantz, Terry D. "Intrusion Detection Update Forecast." Office of INFOSEC Research and Technology, December 2001

45. (U) [redacted] "SNORT:Intrusion Detection for Small Networks," *Tech Trend Notes*, Winter 2002

of the palm, face, iris, retina, voice, hand, finger, signature or keystroke. Other less viable technologies include those involving gait, odor and ear shape. The biometrics technology in general is evolving into a basis for highly secure identification and verification. Supporters believe that federal, state and local governments, the military, and the commercial marketplace all are recognizing its value and will benefit from adoption of the technology.

(U) Proposed applications include using Smart cards in conjunction with biometrics to improve a system's Identification and Authentication (I&A) function. Biometric data from a retina or thumbprint stored on a card can be compared with the data from a biometric input device to authenticate a user. A disadvantage of this approach to a solution is that a primary goal of biometrics is to reduce reliance on cards, not to continue their use. In addition, biometrics are being applied to address the security needs of wireless customers, using fingerprint scanners embedded in handheld equipment. Companies are also developing biometric encryption methods and techniques for securing key using the technology. Potential applications are numerous. However, social acceptance with attendant privacy and ethical concerns remains a major hurdle which will not soon disappear as an issue.[47]

46. Bury, Lawrence J. "Biometrics," Office of INFOSEC Research and Technology, November 2001.
47. Bury, Lawrence J. "Biometrics," Office of INFOSEC Research and Technology, November 2001.

(U) Market Analysis

(U) Worldwide (WW) expenditures for IT security, which enables privacy and is integral to any degree of meaningful privacy, are already substantial, and will continue growing in coming years. Although in the first half of 2002, enterprises tended to continue postponement of large IT projects, including security, IDC believes that this trend will be reversed over the next few years. Data on spending growth in three representative areas of the IT security market (Information Security Services, Internet Security Software, and Wireless and Mobile Security Software) follows.

(U) Information Security Services

(U) Just in the Information Security Services sector alone, the worldwide growth rate between 2001 and 2006 is projected to be 23.7 percent, with the Americas experiencing a somewhat slower percentage increase during the period. (See Table 1 below.) One significant factor in increased U.S. security expenditures has been corporations' and other organizations' efforts to comply with such privacy legislation as Gramm-Leach-Bliley and HIPAA. Fueling the growth in spending, as new technologies appear (e.g., wireless), they bring along with them security holes and privacy concerns which are a worldwide force for acquisition of new services and development of innovative solutions.[48]

Table 1: WW Information Security Services Spending by Region, 2001-2006 ($M)

	2001	2002	2003	2004	2005	2006	2001-2006 CAGR (%)
Americas	4,486	5,347	6,483	7,948	9,864	12,182	22.1
Europe, Middle East, Africa	2,658	3,277	4,089	5,174	6,468	8,039	24.8
Asia/Pacific	881	1,103	1,397	1,794	2,316	2,994	27.7
Worldwide	8,025	9,727	11,969	14,915	18,649	23,216	23.7

Note: Data includes consulting, implementation, management, and response services, but does not include revenue from hardware and software sales.

Source: IDC, 2002

48. (U) Carey, Allan. "Worldwide and U.S. Information Security Services: Midyear Forecast Update, 2002." *IDC Bulletin #27878*, September 2002.

(U) Internet Security Software

(U) In the Internet security software sector, worldwide revenue totaled about $6 billion in 2001, an increase of 18 percent over the previous year. (Nevertheless, the effects of 9/11 on security software spending were not as great as one would have expected, since heavy physical security spending probably lessened the layout of funds for upgrades in computer security.) IDC believes that the 2001 figure will increase to $14.2 billion by 2006, with Security 3A software accounting for the largest increase of a 22 percent CAGR (Compound Annual Growth Rate) to approximately $6 billion.[49] Security 3A is comprised of authentication (includes PKI), authorization, and administration. Firewall/VPN, encryption, and Intrusion Detection software revenue is also projected to grow significantly, as indicated in Table 2. The five leading vendors of Internet security software products in 2001 were Symantec (with 12 percent of the market), Check Point Software Technologies, Network Associates, Computer Associates, and IBM. (See Appendix II.)

(U) Table 2 - WW Internet Security Software Revenue by Segment, 2000-2000($M)

	2000	2001	2002	2003	2004	2005	2006	2001-2006 CAGR (%)
3A	2,005.2	2,212.7	2,633.1	3,212.3	3,951.2	4,899.4	5,977.3	22.0
Firewall/VPN	736.0	894.6	1,010.8	1,132.1	1,268.0	1,407.5	1,548.2	11.6
Secure Content Management	1,652.4	2,012.7	2,455.3	2,970.9	3,535.7	4,136.4	4,799.2	19.0
Encryption	197.3	227.1	247.6	277.3	313.3	344.7	379.1	10.8
IDnA	467.7	619.6	774.5	937.2	1,096.5	1,261.0	1,450.1	18.5
Total	5,058.5	5,966.7	7,121.3	8,529.8	1,064.7	12,048.9	14,153.9	18.9
Growth		18.0	19.4	19.8	19.2	18.5	17.5	100.0

Source: IDC, 2002

(U) Wireless and Mobile Security Software

(U) The security flaws related to wireless and mobile technology are receiving today as much, if not more, attention than any other area of concern to privacy advocates. IDC, in a study of the mobile security market in which they include wireless products, forecasts worldwide revenue growth for security software of nearly 70 percent CAGR by 2006. Security 3A software and secure content management will make up 70 percent of the spending by 2006, but Intrusion Detection and Vulnerability Assessment software will have shown the fastest CAGR of 134 percent, as shown in Table 3.

49. (U) Burke, Brian E., et al. "Worldwide Internet Security Software Market Forecast and Analysis, 2002-2006: Vendor Views." *IDC Bulletin #27639*, July 2002.

Table 3: WW Mobile Security Software Revenue by Segment, 2000-2006 ($M)

	2000	2001	2002	2003	2004	2005	2006	2001-2006 CAGR (%)
Security 3A	12.2	22.7	37.9	66.0	121.8	211.4	368.6	74.6
Firewall/VPN	14.8	22.4	35.4	56.6	82.4	112.6	139.3	44.2
Secure Content Management	8.2	14.0	26.9	53.2	109.0	209.8	362.7	91.7
Encryption	11.7	15.0	21.0	31.3	46.3	64.9	89.2	42.9
Intrusion Detection and Vulnerability Assessment	0.0	1.2	4.6	9.3	21.9	50.3	86.7	134.0
Total	46.9	75.3	125.7	216.4	381.4	648.9	1046.	69.3
Growth	NA	60.7	66.9	72.2	76.2	70.2	61.3	

(U) Over the past year, various attempts to address security shortcomings in wireless technology have been announced by security firms in response to highly critical evaluations of weak privacy protection from Academia, Government and industry. Information on some of these efforts follows:

• (U) In October 2001 Columbitech, a Swedish company, released its VPN for wireless systems which is based on Wireless Transport Layer Security (WTLS), an industry standard protocol. In March 2002, in conjunction with Diversinet, Columbitech unveiled Passport Wireless VPN, which joins the former's wireless PKI technology with its own wireless VPN product. Then in September 2002, the company announced a further enhancement, replacement of 3DES (Triple Data Encryption Standard) with AES (Advanced Encryption Standard).

• (U) In May 2002, Symbol Technologies announced AirBEAM Safe, based on Columbitech encryption technology. The product offers data encryption across wireless circuits, including both 802.11b LANs and cellular networks. The DOS client, a new feature of Columbitech's above September 2002 initiative, is an integrated component of AirBEAM Safe.

• (U) In July 2002, Fortress Technologies and DTNet agreed to cooperate in the area of broadband wireless networks. DTNet will install and service the partnership's products, while Fortress will provide the wireless privacy features of the package, which includes encryption/decryption and access control.[50] The U.S. Army recently picked a Fortress WLAN product for its combat service support network.

• (U) Also in July 2002, SIGABA (TM) Corp. announced a new offering designed to provide secure WLAN Email. The product's Key Server provides Email encryption, and its Plug-in provides authentication.

• (U) In September 2002, Open Computing Platforms (OCP) announced "Secure America," wireless surveillance and security systems, which will carry surveillance data over

50. (U) "Fortress Technologies and DTNet Sign Reseller Agreement," *Business Wire*, 11 July 2002.

secure wireless networks made possible, the vendor claims, by protocols which go well beyond that of WEP encryption.

• (U) Also in September 2002, Bluesocket launched its Homeland Wireless Security Initiative (HWSI). Blue Socket, which already provides its Wireless Gateway products to local, state and federal agencies (including the National Security Agency), is collaborating with the IEEE and IETF to achieve interoperability, greater security, and universal application by means of standards compliance. [51]

51. (U) "Bluesocket Launches 'Homeland Wireless Security Initiative'," *InTernet Wire*, 9 September 2002.

(U) NSA Related Activities

(U//~~FOUO~~) Since its establishment in 1952, NSA has periodically had to make major adjustments in areas where aspects of privacy were involved. In the 70s, Congressional investigations of abuses involving monitoring of the communications of U.S. citizens resulted in the passage of the Foreign Intelligence Surveillance Act (FISA) and the implementation of executive orders and directives, all of which were designed to ensure that the rights, including privacy, of U.S. persons are respected. Since that time, the Agency has scrupulously avoided any activity which would violate either the law or its own directives written to ensure compliance. Ironically, the Agency has sometimes received criticism from users of its SIGINT product who believe that NSA has gone beyond what the law requires and has been too zealous about privacy protection for U.S. persons.

(U//~~FOUO~~) In the aftermath of 9/11, civil liberties groups have resisted a widening of governmental surveillance powers, on the basis that such an expansion will jeopardize privacy rights and that existing authority is adequate to protect against the terrorist threat. Technological advances only exacerbate the controversy. As surveillance capabilities, such as the FBI's DCS1000 system, create additional opportunities to thwart terrorist and other hostile threats, privacy concerns are heightened. Although most expressions of concern are directed at the FBI, NSA is not spared. The ongoing debate about the interpretation of changes to the provisions of FISA, found in the PATRIOT Act, may also impact NSA. Congress and the public want protection from future terrorist attacks, but insist that innocent individuals' right to privacy be respected. With this in mind, DIRNSA publicly broached the subject of legislative changes affecting NSA's charter when he appeared before the Joint Inquiry Committee on 17 October 2002.

(U//~~FOUO~~) Privacy issues also have implications for NSA in ways that are not directly related to accomplishment of its mission as an organization. There are thousands of people employed by the Agency who are faced with the same everyday threats to their privacy and anonymity as the public at large. NSA employees, for example, sometimes use wireless devices, or are subject to biometric examination or surveillance. Personal information transmitted over a WLAN, or biometric data used in construction of a personal profile, could come into the possession of careless or unethical individuals who have no regard for the privacy of others. In some instances, only the individual employee would be harmed. If it is a case of classified or otherwise sensitive NSA information that has fallen into the wrong hands, however, NSA's organizational "privacy" has also been violated.

(U//~~FOUO~~) Since its founding in 1952, NSA has struggled to maintain its anonymity and the "privacy" of its information. When an individual, is determined to release NSA information to parties with whom the Agency does not want it shared, there often is little that can be done to prevent it from happening. In some instances, the violation has nothing to do with IT. The offender may simply have received a briefing or heard a report passed by word of mouth, which he passes on to an unauthorized individual. In other cases, easy access by cleared Intelligence Community personnel to terminals providing a SIGINT product retrieval capability makes possible unauthorized release of NSA's private information. Such a release also damages the Agency's anonymity. Unlike most organizations, which would want their successes known to the public, NSA will do

everything it can to avoid it. When a critical piece of intelligence is publicly attributed to NSA, it is highly possible that a vital and fragile source will be lost.

(U//~~FOUO~~) Although there is little the Information Assurance (IA) Directorate or the IA Research Associate Directorate can do about intentional security/privacy violations by cleared personnel, there is significant internal research being done on several fronts to fill gaps arising from, but not adequately addressed, during the development phase of new technologies. For example, there is a team in the Research organization dedicated to the solution of wireless multimedia security problems. NSA has been specifically asked by OSD to assist in the development of a wireless security strategy for DoD. Other Research teams deal with cryptography (Public Key and Symmetric), as well as Key Management Infrastructure. In 2001, the Research organization publicly announced the availability of SELinux (Security Enhanced Linux) for download. SELinux is a key component of NSA's NetTop project which will give NSA analysts secure simultaneous access to classified and unclassified (e.g., Internet) information, using a single physical computer. These are just a few of the many tasks NSA's Research organization--often in cooperation with industry, universities, and other U.S. Government research entities--has undertaken to improve the security (and privacy) posture of computer users inside and outside of government.

(U//~~FOUO~~) New technologies are not an unmixed blessing for intelligence or other government agencies. As Whitfield Diffie, Sun Microsystems chief security officer, has pointed out, typically security technology does not keep pace with other IT developments.[52] Technologies such as WLAN are often accompanied by gaping security holes not easily remedied. Aggravating this problem for security organizations such as NSA's IA Directorate, relaxed export restrictions and technology transfer programs mandated by Congress--while frequently offering potential benefits to the U.S. national economy and to computer users around the world seeking enhanced privacy--also can complicate at least indirectly the conduct of the Agency's IA mission. The more another nation learns about securing its own communications, the greater its potential capability for a successful attack on those of others.

52. (U) "Technology Trends Are Pushing U.S. Intelligence Agencies Toward 2nd-Generation Public-Key Encryption and Toward Cyberwarfare." *Washington Internet Daily*, 8 August 2002.

(U) Conclusions

(U) As new IT technologies arrive on the scene, they almost inevitably bring with them at least the potential for privacy problems. Companies rush to get their product on the market to secure a foothold, and postpone repairing security flaws which in many instances they know, or assume, exist. Privacy-protection shortcomings are often apparent to users from the moment a product is released, or even announced with preliminary details. Because the new product fills a significant need or because it is easier to use than its predecessor, customers risk deploying and using it, thinking the threat to other users is greater. Nevertheless, user awareness of security flaws results in rising concern about loss of privacy, which in turn leads to a demand for a solution. Even the solution itself is sometimes found to be inadequate, giving rise to a need for further research and development.

(U) Many experts and civil libertarians believe that technological solutions alone are not the answer, especially in the face of a skilled and determined effort to violate the privacy of computer users. They argue that careful and faithful use of encryption and other privacy-protection measures help limit the danger, but that strong enforcement of existing laws and passage of new ones in response to emerging threats, are essential. Once new legislation is in place, the risk to personal privacy is substantially reduced, since many hackers--at least those subject to the law--are not willing to take a chance on incurring the penalties provided. NSA also benefits from effective privacy legislation inasmuch as its employees receive the protection afforded by the law. Sensitive information about Agency workers or about the Agency itself that fell into the wrong hands in the absence of privacy statutes could easily harm NSA as an organization.

(U//~~FOUO~~) Although not a threat to NSA anonymity, wide availability of privacy-enhancing technologies has the potential to affect negatively the performance of the Agency's mission. When U.S. encryption export restrictions were relaxed in response to the urging of advocates of increased privacy for computer users worldwide and of IT companies eager to make sales abroad, there were concerns that it would become harder (and, by extension, more expensive) for the Agency to produce foreign intelligence, as NSA's former Deputy Director warned in 1999 remarks to a Congressional Committee in open session. Sales abroad of U.S. encryption will continue to increase the challenge for NSA analysts.

(U//~~FOUO~~) Not just NSA's SIGINT mission can be adversely affected by the availability of commercial privacy-protection products, however. In recent years, U.S. Government agencies--including DoD and the Intelligence Community--have been buying increasing amounts of commercially produced security products. When one of these products is acquired by a Government agency, careful and thorough testing and evaluation is necessary to ensure the absence of IA vulnerabilities. Notwithstanding the possible negative consequences of using commercial privacy-protection products, cost savings to the Government have on balance made commercial purchases a desirable option.

(U//~~FOUO~~) Finally, the IA and IA Research elements of the Agency will continue to monitor the appearance of new communications technologies with respect to their vulnerabilities. Where there are security problems, as in Wireless transmission, NSA will devote resources to share in

the effort to resolve shortcomings. Despite the increasingly prominent role of the private sector in developing security/privacy solutions, NSA's responsibilities in the more critical security areas will remain dominant.

(U) Appendix I

(U) EPIC Online Guide to Practical Privacy Tools (Updated June 2002)

(U) Disclaimer: EPIC does not lobby for, consult, or advise companies, nor do we endorse specific products or services. This list merely serves as a sampling of available privacy-enhancing tools. If you have a suggestion for a tool that you believe should be included, or if you have comments to share regarding one or more of the tools that are already listed, send e-mail to info@epic.org. If you have questions about a tool on this page, visit the affiliated company or individual's website for more information.

(U) Featured Tool: Privacy Analysis of your Internet Connection From Privacy.net, the consumer information organization. Analyzes many different types of information that is collected about you when you visit a Web site, such as whether cookies are accepted, what site you linked to the page from, and the date and time as set on your computer.

(U) Snoop Proof Mail

1on1. Secure mail with encrypted attachments, digital signatures, etc.

CryptoHeaven (see also under "secure instant messaging").

Ensuredmail. Easy-to-use encryption software that protects your email and attachments.

HushMail. Web-based secure email.

KeptPrivate. Web email client accessible over an SSL connection.

Mail2Web. Check your mail securely and privately on the road (or on your cellular phone). Safe-email.net.

SafeMessage. Encrypted messages, delivery status, and automatic shredding.

SoftClan E-Cryptor.

Stealth Message. Web-based e-mail privacy with option to self-destruct.

Ziplip.com. A free e-mail service that will scramble, lock, and then shred email.

(U) Anonymous Remailers

@nonymouse.com . Also offers anonymous Web surfing and newsgroup posting. Available in both German and English.

COTSE offers **Anonymous Remailer** services to members.

Jack B. Nymble.

Riot Anonymous Remailer (also available in Spanish and Italian).

Ultimate-Anonymity.org. Anonymous e-mail and web surfing, Usenet posting, newsgroups, IRC/ICQ and chat rooms.

André Bacard's **Anonymous Remailer FAQ**.

Surf Anonymously

The Anonymizer.

BrowserSpy. Provides detailed information about what your browser supports and reveals.

BrowsInfo. See what can be discovered about your browser.

The Cloak. Free anonymous web-surfing.

Fogbank-now. Firewall-protected remote Internet browser. Also offers encrypted e-mail and other services.

Freedom WebSecure.

GoProxy.

Guardster.

I Can See You. Program from anonymizer.com shows you the information your browser reveals. (NOTE: this program runs a Javascript file that may bring up a virus alert. The file is safe; however, if you experience any further problems, please contact the web administrators at anonymizer.com.)

IDzap. Anonymous surfing and web hosting.

JAP.

Ponoi. Anonymous web-browsing, encrypted file storage, password storage, and cookie management.

Rewebber.

Surfprivately.

Silenter. Free anonymous surfing through a proxy.

(U) HTML Filters

AOTop. Stops unwanted ad banners and pop-ups with a configurable ad-obfuscating tool for visual privacy protection.

Don't Panic. Prevent browser pop-ups, clear cache and cookies, and more.

InfoWorks Technology Company offers products to get rid of pop-ups, erase history, and others.

Internet Eraser.

Junkbuster (Windows/UNIX). The Internet Junkbuster Proxy blocks unwanted banner ads and protects your privacy from cookies and other threats.

Orangatango's VirtualBrowser. Surf privately, kill pop-up ads, prevent spam, encrypt surfing, filter content, and avoid online fraud.

PC Privacy Protection Program.

Personal Sentinel. Block third party cookies, remove privacy threats, filter unwanted content, and block unwanted ads.

Proxomitron (Windows). Get the web-surfing experience that you want.

Smasher (Windows). Block cookies and pop-up windows, squash web bugs, and more.

Surfer Protection Program.

(U) Cookie Busters

Burnt Cookies (for Internet Explorer on Windows platform).

Cookie Cruncher (Windows).

Cookie Crusher (Windows).

Cookie Cutter 1.0 (for Netscape on Macintosh platform). Direct download.

Cookie Jar (UNIX).

MagicCookie Monster (for Netscape on Macintosh platform).

(U) Voice Privacy

PGP Phone (Mac and Windows 95). Turn a PC into a secure telephone.

Mac international distribution (direct download from Norway).

web.mit.edu/network/pgpfone

Speak Freely.

(U) Email and File Privacy

GnuPG - the GNU Privacy Guard.

Message Sentinel. Analyzes incoming e-mail and blocks privacy threats.

PeepLock offers products for file encryption, message encryption, and e-mail security.

Pretty Good Privacy (PGP). Protect privacy of electronic mail and files.
Available for most machines.

Distribution from MIT.

International PGP **Home Page**.

International distribution from Finland.

Private Idaho

"Where to Get PGP FAQ" via email. Mail **ftp-request@netcom.com** with the line SEND mpj/getpgp.asc.

PGP Users List and Reference.

André Bacard's **PGP FAQ.**

(U) Secure Instant Messaging

CryptoHeaven. Secure instant messaging, as well as secure e-mail, file sharing,

and online storage.

Imici. OpenSSL encrypted instant messaging.

IMpasse. Encrypts AIM, Yahoo! and MSN messages.

Project SCIM: Secure Cryptographic Instant Messaging. Runs on many different platforms.

PSST. Encrypted instant message software for Windows and Linux.

Secure Shuttle Transport. Encrypted instant messaging, FTP, text chat, voice chat, and more.

Sonork. Set up and control your own Instant Messaging system.

(U) Web Encryption

Check the strength of the crypto in your browser.

Fortify (Windows 95/NT/UNIX). Upgrades weak international version of Netscape into strong 128-bit version. Available worldwide.

(U) Telnet Encryption

F-Secure SSH. Secure Telnet for Mac/Windows/UNIX (Finland).

OpenSSH.

MacSSH (Macintosh PowerPC).

TTSSH (Windows).

(U) Disk Encryption

Encrypt your entire hard drive.

Cryptdisk (Mac).

SafeBoot (Windows).

Scramdisk.

(U) Disk/File Erasing Programs

Completely erase files so that they cannot be recovered or undeleted.

Burn 2.5 (Macintosh).

Clean It Up!

DiskVac (Windows).

E3 Security Kit.

Eraser 3.5.

Evidence Eliminator (Windows).

File Wiper for DOS (direct download).

Wintracks (Windows). Available in English and French.

(U) Privacy Policy Generators

OECD Privacy Policy Generator.

(U) Password Generators

PW-Gen. Hardly predictable password generator.

(U) Firewalls

BlackICE Defender.

BrickHouse. For Mac OS X.

(U) Personal Firewall

Tiny Personal Firewall.

ZoneAlarm. Freeware alternative.

(U) Other Resources

Cryptoarchive (mirror site).

"Cryptographic software solutions and how to use them."

Crypt0graphy Research Labs. Links to cryptographic and other resources.

OkayCash. Shop online without a credit card.

PCWorld: 34 steps you can take to reclaim your online privacy. (June 2002)

Privacy Communications, Inc. (PrivCom). Encrypted faxes and voicemail.

Shields UP! Internet Connection Security Analysis.

SpamEx: Disposable E-mail Address Service.

SpyCop. Detects an ever-growing number of "spy programs" which monitor computer usage.

Who's Watching Me? Snooper Detector. Checks your system for "snoopers," or software that is installed on a computer to record actions and events.

(U) Disclaimer: EPIC does not lobby for, consult, or advise companies, nor do we endorse specific products or services. This list merely serves as a sampling of available privacy-enhancing tools. If you have a suggestion for a tool that you believe should be included, or if you have comments to share regarding one or more of the tools that are already listed, send e-mail to info@epic.org. If you have questions about a tool on this page, visit the affiliated company or individual's website for more information.

EPIC Privacy Page | EPIC Home Page

Last Updated: June 13, 2002 Page URL: http://www.epic.org/privacy/tool s.html

(U)Appendix II

IDC Internet Security Software Vendors and Revenue Figures for 2000 and 2001

Worldwide Internet Security Software Revenue by Vendor, 2000 and 2001 ($M)

	2000	2001	2001 Share (%)	2000-2001 Growth (%)
Symantec Corp.	589.7	718.0	12.0	21.7
Check Point Software Technologies	418.1	531.0	8.9	27.0
Network Associates	440.8	497.0	8.3	12.8
Computer Associates Intl.	612.0	435.0	7.3	-28.9
IBM	290.0	307.0	5.1	5.9
Trend Micro	191.0	250.0	4.2	30.9
Internet Security Systems	161.5	177.0	3.0	9.6
RSA Security	192.5	165.0	2.8	-14.3
Entrust Technologies	115.1	88.1	1.5	-23.5
Hewlett-Packard	81.5	84.5	1.4	3.8
Microsoft Corp.	58.8	83.8	1.4	42.5
Netegrity	45.7	79.9	1.3	74.8
Baltimore Technologies	74.3	70.6	1.2	-5.0
Sun Microsystems	78.0	69.1	1.2	-11.4
BindView Corp.	77.5	69.0	1.2	-11.0
Fujitsu Ltd.	42.5	50.1	0.8	17.8
Novell	45.8	50.0	0.8	9.2
Secure Computing Corp.	34.7	48.4	0.8	39.5
SurfControl	27.0	46.1	0.8	70.7
F-Secure Corp.	40.1	44.1	0.7	10.0
Hitachi Ltd.	42.5	44.1	0.7	3.8
Groupe Bull	39.6	43.4	0.7	9.4
Sophos	27.0	41.4	0.7	53.3
PentaSafe Security Technologies	16.7	39.0	0.7	134.1

NetIQ	23.7	39.0	0.7	64.5
Websense	17.4	35.6	0.6	104.6
AOL	25.6	31.5	0.5	23.0
Ubizen	23.0	31.0	0.5	34.8
Sybari Software	16.0	30.0	0.5	87.5
BMC Software	28.0	30.0	0.5	7.1
Panda Software	22.0	28.0	0.5	27.3
Tumbleweed Communication	24.0	27.0	0.5	12.5
Cisco Systems	24.1	26.1	0.4	8.3
Norman ASA	15.0	22.3	0.4	48.9
Ahnlab	13.3	20.2	0.3	51.8
Rainbow Technologies	12.3	20.0	0.3	62.6
Gemplus International S.A.	10.6	20.0	0.3	88.7
ValiCert	9.5	19.9	0.3	109.5
SSH Communications Security	14.5	18.0	0.3	24.1
Enterasys Networks	10.5	18.0	0.3	71.4
Systor AG	13.0	16.8	0.3	29.2
Certicom Corp.	15.2	15.2	0.3	-0.3
Oblix	14.0	15.0	0.3	7.1
VeriSign	5.8	15.0	0.3	157.6
Utimaco Safeware AG	7.0	15.0	0.3	114.3
Aventail	10.7	15.0	0.3	40.3
StoneSoft Corp.	10.0	13.0	0.2	30.2
SilentRunner	8.7	13.0	0.2	49.4
ZoneLabs	2.4	12.8	0.2	433.3
Entegrity Solutions	8.6	12.1	0.2	40.6
Unisys Corp.	11.9	11.1	0.2	-6.7
Arcot Systems	6.5	10.0	0.2	53.8
Keyware	7.0	10.0	0.2	42.9
Tripwire Security	8.0	10.0	0.2	25.0
N2H2	7.0	9.3	0.2	32.9
Elron Software	11.0	9.1	0.2	-17.3

8e6 Technologies	7.0	8.6	0.1	23.0
Intrusion.com	12.8	8.2	0.1	-35.8
Rulespace	5.5	8.0	0.1	45.5
Aladdin Knowledge Systems	5.0	7.6	0.1	52.0
Sanctum	3.5	7.5	0.1	114.3
Access 360	7.0	7.4	0.1	6.2
Vasco	6.0	7.4	0.1	23.0
Cybersafe	12.4	7.0	0.1	-43.7
NEC Corp.	6.6	7.0	0.1	4.9
Candle Corp.	6.0	6.7	0.1	11.9
Finjan Software Ltd.	6.0	6.5	0.1	8.3
Consul Risk Management	0.0	6.0	0.1	NA
Group Software	3.0	6.0	0.1	100.0
Recourse Technologies	4.0	6.0	0.1	50.0
Clearswift Corp. .	2.0	5.0	0.1	150.0
Cylink Corp.	7.6	5.0	0.1	-34.2
Entercept Security Technologies	2.0	5.0	0.1	150.1
nCircle	0.0	5.0	0.1	NA
Spyrus	0.0	5.0	0.1	NA
Sygate Technologies	2.0	5.0	0.1	150.0
Kyberpass	2.1	5.0	0.1	138.1
Hauri	2.7	4.2	0.1	55.9
Business Layers	2.0	4.0	0.1	100.0
netForensics	0.0	4.0	0.1	NA
RedCreek Communications	5.0	4.0	0.1	-20.0
Beta Systems Software AG	3.3	3.5	0.1	6.1
Protegrity	1.3	3.4	0.1	172.0
Marshall Software	1.8	3.1	0.1	72.6
BioNetrix	0.0	3.0	0.1	NA
Citadel Technology	2.0	3.0	0.1	50.0
Phaos Technology	2.2	2.9	0.0	31.8
V-One Corp.	2.2	2.5	0.0	15.2

Korea Information Engineering Services	0.0	2.3	0.0	NA
Astaro	0.0	2.0	0.0	NA
Citrix Systems	1.2	1.6	0.0	35.3
Promia	0.0	1.3	0.0	NA
Proginet Corp.	1.0	1.2	0.0	24.3
Kavado	0.0	1.0	0.0	NA
Safewww	0.0	1.0	0.0	NA
NovaStor	0.8	0.9	0.0	22.5
Open Systems Management Ltd.	0.0	0.9	0.0	NA
Volera	0.0	0.5	0.0	NA
Tempest Software	0.0	0.5	0.0	NA
Steganos	0.0	0.5	0.0	NA
SuSE Linux AG	0.0	0.5	0.0	NA
Zixlt	0.0	0.4	0.0	NA
Macro 4	0.2	0.1	0.0	-52.8
Enlighten Software Solutions	1.6	0.1	0.0	-96.4
Sybase	1.4	0.0	0.0	-100.0
Subtotal	4,307.9	4,838.0	81.1	12.3
Other	750.6	1,128.7	18.9	50.4
Total	5,058.5	5,966.7	100.0	18.0

(U) Bibliography

(U) "Bluesocket Launches 'Homeland Wireless Security Initiative'," *InTernet Wire*, 9 September 2002.
(U) Borisov, Nikita et al. "Security of the WEP Algorithm," University of California Paper, July 2001.
(U) Brewin, Bob and Verton, Dan. "DoD IT Projects Come Under Fire," *Computerworld*, 16 May 2002.
(U) Burke, Brian E., et al. "Worldwide Internet Security Software Market Forecast and Analysis, 2002-2006: Vendor Views," *IDC Bulletin #27639*, July 2002.
(U//~~FOUO~~) Bury, Lawrence. "Biometrics, A Technology Forecast," Office of INFOSEC Research and Technology, November 2001.
(U//~~FOUO~~) Cameron, William. "Public Key Infrastructure, A Technology Forecast," Office of INFOSEC Research and Technology, August 1999.
(U) Carey, Allan. "Worldwide and U.S. Information Security Services: Midyear Forecast Update, 2002," *IDC Bulletin #27878*, September 2002.
(U) ---. "Worldwide Information Security Services Forecast, 2001-2006," *IDC Report #26899*, April 2002.
(U) Chang, Nancy. "The USA Patriot Act: What's So Patriotic About Trampling on the Bill of Rights?," *Center for Constitutional Rights*, November 2001.
(U) "Consumer Benefits of Today's Digital Rights Management (DRM) Solutions: Hearings before the Subcommittee on Courts, the Internet, and Intellectual Property of the Committee on the Judiciary, House of Representatives, 107th Congress, Second Session, 5 June 2002," Serial No. 72.
(U) Costello, Sam. "Microsoft Offers Palladium Details," *IDG News Service*, 29 July 2002.
(U) Cranor, Lorrie and Langheinrich, Marc, et al. "The Platform for Privacy Preferences 1.0 (P3P 1.0 Specification)," Worldwide Web Consortium, 16 April 2002.
(U) Cranor, Lorrie. "The Role of Privacy Advocates and Data Protection Authorities in the Design and Deployment of the Platform for Privacy Preferences," Remarks at the Twelfth Conference on Computers, Freedom, and Privacy, San Francisco, April 16-19, 2002.
(U) David, Natasha and Chee, Wilvin. "Asia/Pacific (Excluding Japan) Security Software Market Forecast and Analysis," *IDC Report #AP321332J*, April 2002.
(U) "Digital Rights Management and Privacy," *Electronic Privacy Information Center*, 11 July 2002.
(U) Edwards, Mark Joseph. "Severe Vulnerability in Internet Explorer SSL," *Wininfo InstantDoc #26245*, 13 August 2002.
(U) Ellison, Carl and Schneier, Bruce. "Ten Risks of PKI: What You're Not Being Told about Public Key Infrastructure," *Computer Security Journal, Volume XVI, Number 1*, 2000.
(U) "EPIC Online Guide to Practical Privacy Tools," *Electronic Privacy Information Center*, 18 April 2002.
(U) "Fortress Technology and DTNet Sign Reseller Agreement," *Business Wire*, 11 July 2002.
(U) Girard, John and Pultz, Jay. "The Pros and Cons of Building a VPN," *Gartner Research Note*, 30 August 2001.
(U) Givens, Beth. "Eight Reasons to be Skeptical of a Technology Fix for Protecting Privacy," *Privacy Rights Clearinghouse*, 14 October 2000.

(U) Green, Joe and Gaw, Jonathon. "Security and Privacy: Inextricably Linked," *IDC Bulletin #CA0751EJ*, April 2002.
(U) Greene, Thomas C. "Do-it-yourself Internet Anonymity," *The Register*, 1 July 2002.
(U) "Guide to Online Privacy, Chapter Three: Existing Privacy Protections," *Center for Democracy and Technology*, 2000.
(U) Harrison, Ann. "Peer-to-Peer Anonymization," *Network World Peer-to-Peer Newsletter*, 24 July 2002.
(U) "Hearing on the Reauthorization of the Federal Trade Commission," *Center for Democracy and Technology*, 17 July 2002.
(U) Hudson, Sally and Christiansen, Christian A. et al. "Mobile Security Software Forecast, 2002-2006," *IDC Bulletin #27354*, June 2002.
(U) Karygiannis, Tom and Owens, Les. "Draft: Wireless Network Security, 802.11, Bluetooth and Handheld Devices," *NIST Special Publication 800-48*, 29 July 2002.
(U) Kearns, Dave. "I'm from Microsoft, and I'm Here to Help You," *Network World*, 15 July 2002.
(U//~~FOUO~~) Lantz, Terry D. "Intrusion Detection Update Forecast," Office of INFOSEC Research and Technology, December 2001.
(U) Ledford, Jerri. "Ensuring Privacy and Security for Medical Systems," *Faulkner Information Systems*, February 2002.
(U) Mantin, Istil et al. "Weakness in the Key Scheduling Algorithm for RC4," Paper Presented at Toronto Cryptographic Conference, August 2001.
(U) Pescatore, John. "Identity Services Do Not End Privacy Online," *Gartner Commentary*, 29 March 2002.
(U) Pescatore, John and Wheatman, Vic. "Management Update: Gartner's Information Security Hype Cycle Helps to Cut Risks," *InSide Gartner*, 28 November 2001.
(U) ---. "Secure Socket Layer Sometimes Isn't," *Gartner Research Note*, 3 April 2002.
(U) Poulson, Kevin. "DEA Data Thief Pleads Guilty," *Security Focus Online*, 7 August 2002.
(U) "Privacy and Security on your PC," *Extreme Tech*, 28 May 2002.
(U) "Proposal for a Directive of the European Parliament," Commission of the EC, 30 May 2002.
(U) Rickard, Neil. "Do MPLS VPNs Deserve to be Called Private?," *Gartner Research Note*, 5 March 2002.
(U) Rohde, Laure. "Study: SSL Encryption Weaker in Europe than in U.S.," *IDG News Service*, 3 April 2002.
(U) [redacted] "SNORT:Intrusion Detection for Small Networks," *Tech Trend Notes*, Winter 2002.
(U) Shields, Clay. "Statement of Research Interests," Georgetown University, 2002.
(U) Stubblefield, Adam. "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP," *AT&T Labs Technical Report TD4ZCPZZ, Revision 2*, 21 August 2001.
(U) "Technology Trends Are Pushing U.S. Intelligence Agencies Toward 2nd-Generation Public-Key Encryption and Toward Cyberwarfare," *Washington Internet Daily*, 8 August 2002.
(U) U.S. Supreme Court, Watchtower Bible & Tract Society v. Village of Stratton, 17 June 2002.
(U) Walton, Timothy J. "Internet Attorney," *Internet Privacy Law*, 2000.
(U) "Welcome to the Safe Harbor," U.S. Department of Commerce, 2000.
(U) Wheatman, Vic. "Corporate Privacy," *Gartner Letter from the Editor*, 23 October 2001.
(U) ---. "Public Key Infrastructure 1 H02 Magic Quadrant," *Gartner Research Note*, 14 February 2002.

(b)(3)-P.L. 86-36

(U) ---. "Questioning the Value of Digital Signatures," *Gartner Commentary*, 17 June 2002.
(U) "Wireless Location," *Center for Democracy and Technology*, 30 July 2001.
(U) Wright, Matthew and Adler, Micah et al. "An Analysis of the Degradation of Anonymous Protocols," Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS 2002), February 2002.