The Encryption Debate in Plaintext: National Security and Encryption in the United States and Israel

Barak D. Jolish

Cooley Godward, LLP
One Maritime Plaza, 20th Floor, San Francisco, CA 94111-3580, USA
bjolish@cooley.com, bjolish@yahoo.com

Abstract. The United States has traditionally restricted the export of strong encryption so as to keep the technology from criminal or enemy hands. This policy was, however, ineffective–those seeking strong encryption simply turned to non-US sources. Facing mounting legal and legislative challenges from the software industry and free speech advocates, in January of 2000 the Clinton administration finally relented and substantially liberalized its encryption export policy. In an interesting parallel, national security-obsessed Israel has also come to recognize that the security benefits of strict encryption regulation do not justify the economic costs. Indeed, though its regulations are comprehensive, Israel has permitted the export of strong encryption for years. Ultimately, then, the central question is now not whether governments will liberalize their policies, but rather how quickly international competition will force the pace of change.

1 Introduction

Ramsi Yousef was the model of a modern terrorist. Thoroughly ambitious, he traveled the world, planning to blow up American jetliners over Hong Kong, to assassinate the Pope in the Philippines, to bomb an Israeli Embassy in Thailand, and, of course, to detonate a massive explosion that would topple one of the World Trade Center's towers into the other. Such an agenda required formidable organizational skills; Yousef needed to keep track of schedules, targets, and supplies—to say nothing of far-flung networks of co-conspirators and the funds to support his ventures. Like any globetrotting executive, then, Yousef carried a laptop computer, and on this computer he carried encrypted files detailing his agenda.

See Robert D. McFadden, *Out of the Shadows of the World Trade Center Plot*, N.Y. TIMES, Aug. 7, 1995, at B1; *see also* Benjamin Weiser, *Suspect's Confession Cited As Bombing Trial Opens*, N.Y. TIMES, Aug. 6, 1997, at B6.

See MCFADDEN, *supra* note 1, at B1.

See Christopher S. Wren, *Terror Case Hinges On Laptop Computer,* N.Y. TIMES, July 18, 1996, at B3.

Y. Frankel (Ed.): FC 2000, LNCS 1962, pp. 202–224, 2001.

As it happened, this computer played a crucial role in Yousef's downfall. When the bomb chemicals he was mixing in the kitchen sink of his Manila apartment caught
fire, he left the laptop behind in his haste to escape. As FBI Director Louis Freeh recounted in testimony before the United States Senate,

> [w]e were fortunate in that Yousef was careless in protecting his computer password. Consequently, we were able to decrypt his files. . . . Had that fire not broken out or had we not been able to access those computer files, Yousef and his co-conspirators might have carried out the simultaneous bombings of 11 United States airliners, with potentially thousands of victims.

Yet, as Freeh explained, "[m]ost encryption products manufactured today for use by the general public are non-recoverable. This means they do not include features that provide for timely law enforcement access to the plain text of encrypted communications and computer files that are lawfully seized."

Such national security concerns dominated American encryption policy in the twentieth century. Indeed, during this period the United States strictly controlled the export of encryption, and proposed mechanisms to facilitate law enforcement access to domestically encrypted material as well. By the 1980s, however, other concerns had begun to vie for primacy in encryption policy-making. Most influential were the powerful American software industry's claims that strict encryption controls hampered its ability to compete on world markets, and that attempts to handicap encryption's proliferation were in any event bound to fail. Also active were Internet privacy advocates, who stressed that encryption is vital to protecting personal data, and free speech advocates, who contended that encryption code deserves First Amendment protection. Responding to these pressures, in January of 2000 the US government released new regulations substantially relaxing export controls over retail and open source encryption products.

As the fight over US encryption has been exhaustively studied and discussed, it may be interesting to look also at the parallel policy shifts taking place in Israel. Indeed, Israel's encryption dilemma is in many ways an

See id.

Hearing of the United States Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, 96th Cong. (February 4, 1999) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation).

Id.

See WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE, 49-76 (1998) (describing the U.S. government's attempts to control cryptography since World War I).

amplified version of that of the US. On the one hand, Israel's security concerns are amongst the most serious in the world, while on the other its economy is amongst the most reliant on high technology exports. It is therefore significant that, through the recent revision of its encryption regulations, Israel too appears to have concluded that the economic costs of stringent controls outweigh the security threat.

The Israeli and American examples–along with the actions of most other industrialized countries–indicate a clear trend towards more liberal encryption policies. The relevant question over the next decade will thus not be whether encryption will be liberalized, but rather just how quickly international competition will force the pace of change.

Section 2 of this paper will briefly summarize US encryption policy before the reforms of January, 2000, as well as the arguments, legislation, and lawsuits that challenged the status quo. Section 3 will review the new January regulations, and discuss possible ambiguities. Section 4 will introduce the security and economic context in which Israeli encryption policy has evolved. Section 5 will survey Israeli encryption law and regulations, and comment on their implementation. Finally, Section 6 will briefly comment on the future landscape of encryption controls.

2 US Encryption Policy

2.1 Pre-January 14, 2000 US Policy

As discussed in the introduction, members of the American national security establishment–primarily, the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA)–have forcefully argued that strict encryption controls are necessary in order to keep the technology from terrorists and other criminals. In a 1999 report, for instance, the FBI specifically describes the Ramsi Yousef incident, CIA spy Aldrich Ames' Russian handlers instructions that he encrypt his files, and the efforts of child pornographers to encrypt Internet transmissions of illegal photographs.

Successive US administrations have addressed these concerns by: (a) implementing laws restricting the export of strong encryption, (b) forwarding proposals to regulate domestic encryption, and (c) attempting to persuade other countries to control encryption exports.

Export Restrictions. Since 1996, jurisdiction over the export of commercial encryption software has rested with the Commerce Department's Bureau of

FREEH, *supra* note 5.

See, e.g., Encryption: Impact on Law Enforcement, FEDERAL BUREAU OF INVESTIGATION, June 3, 1999 at 6. This report is available on the Internet at <http://www.fbi.gov/library/encrypt/en60399.pdf>.

Export Administration (BXA). The BXA regulates encryption through a licensing scheme under the authority of the Export Administration Act and the Export Administration Regulations. Prior to 2000, the BXA generally required that those wishing to export software comply with a rigorous licensing procedure, and denied such licenses to strong encryption products. In recent years, however, the BXA instituted piecemeal, narrow reforms to the Regulations. In 1998, for instance, the bureau eased controls over 56-bit encryption exports to most countries after a one-time governmental review, and relaxed controls over exports to subsidiaries of US corporations, financial services and medical/health care institutions, and some online merchants. Finally, the BXA has also been quick to promote license exemptions for "recoverable" products, which provide law enforcement "back-door" access to encrypted information.

Attempts to Control Domestic Encryption. Though American encryption policy has never covered the domestic use of encryption, the NSA and FBI have nonetheless consistently pressed for "industry standards" and legislation giving them access to the plaintext of encrypted material. In the early 1990s, for instance, these agencies attempted to convince manufacturers to

See Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996) (Administration of Export Controls on Encryption Products); *see also* United States Munitions List, 22 C.F.R. 121.1 (1997); 22 U.S.C. 2778 (1994) (prescribing administration of the United States Munitions List). The State Department, Defense Department, NSA , and FBI all retain concurrent review authority over encryption export applications.

See Export Administration Act of 1979, Pub. L. No. 96-72, 93 Stat. 503 (codified as amended at 50 U.S.C. app. 2401-2420 (1988 & Supp. III 1991)).

See Export Administration Regulations, 15 C.F.R. 730-774 (1998).

Though until recently 56 bit cryptosystems were considered these encryption schemes "strong," the benchmarks for this term may well have shifted in light of researchers' success in cracking these codes in only a few hours. *See, e.g.*, James Glave, *Code-Breaking Record Shattered*, WIRED.COM (Jan. 19, 1999) <http://www.wired.com/news/news/technology/story/17412.html>.

63 Fed. Reg. 72156 (1998). These reforms followed a series of meetings between high technology industry leaders and members of the US national security establishment. *See Tech Titans Go to Washington*, WIRED.COM (June 9, 1998) <http://www.wired.com/news/news/politics/story/12859.html>.

See id.

incorporate a "Clipper Chip" into their communications products. The Clipper Chip is a semiconductor that encodes and decodes messages using a government-developed algorithm called "Skipjack."

Once operational, the system would allow the government to wiretap otherwise confidential communications. Ultimately, however, the concept of such broad surveillance proved tremendously unpopular, and only a handful of Clipper Chips were ever sold.

Attempts to Control Encryption's Proliferation Abroad. The United States has attempted to convince other countries to adopt measures to control the proliferation of encryption. These efforts have generally met with little success, as illustrated by the Organization for Economic Coordination and Development's (OECD) rejection of US efforts to include government access requirements in its encryption policy guidelines. Recently, however, the U.S. did manage to convince the signatories of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ("Wassenaar Arrangement") to impose some reporting restrictions on the export of encryption with key lengths exceeding 64-bits. Note, however, that while the agreement covers Russia, the United Kingdom and 30 other countries, if does not include encryption-producers such as China, India, South Africa, or Israel.

2.2 Challenges to the pre-January 14, 2000 US policy

The harshest opposition to the government's encryption policies came from US software makers and privacy and free speech advocates. Most influential was the software industry, which by 1999 had invested substantial money and

See generally BRUCE SCHNEIER, *Cryptography Primer, in* THE ELECTRONIC PRIVACY PAPERS 258, 307-13 (Bruce Schneier & David Banisar, ed., 1997) .
See id at 310.
See id.
See SCHNEIER, *supra* note 16, at 317.
See OECD Adopts Guidelines for Cryptography Policy, OECD (March 27, 1997) <http://www.oecd.org/news_and_events/release/nw97-24a.htm>.
An up-to-date version of the agreement may be found at <http://www.wassenaar.org/docs/index1.html>. "Dual use" goods are goods that have both civil and military uses.
See id. at < http://www.wassenaar.org/list/Summary.html>.
See Elizabeth Corcoran, *Encryption Curbs Backed By 33 Nations,* WASHINGTON POST, Dec. 4, 1998 at D1.

effort in political lobbying and campaign contributions. Specifically, the industry claimed that export controls drove those seeking strong encryption to buy products from other countries, a fact that cost US producers billions of dollars. They further noted that US workers were also hurt, as even domestic companies hired independent overseas software developers to create encryption products.

Additional criticism of US policy came from privacy advocates, who argued that encryption products were necessary to protect personal privacy, and free speech advocates, who saw controls as an unconstitutional prior restraint on the First Amendment right to publish.

Though their agendas differed, the above parties were united in their claims that the government's policy stood little chance of significantly controlling criminals' use of encryption. First, they noted that producing encryption algorithms takes few resources; one needs only a computer—or even a pencil and paper—and advanced mathematical training to create an encryption scheme. In fact, sometimes even these skills are not necessary; in early 1999 a 16-year-old Irish high school student named Sarah Flannery developed a new data-encryption algorithm 22 times faster than the popular RSA algorithm used in most business transactions today. Second, reform

See, e.g., Leslie Wayne, *Inside Beltway, Microsoft Sheds Image as Outsider*, N.Y. TIMES, May 20, 1999; Jeri Clausing, *Internet Issues on Front Burner as Congress Returns,* N.Y. TIMES, July 13, 1999.

See, e.g., Immediate Need for Export Control Relief for Software With Encryption Capabilities: Hearing Before the House Committee On The Judiciary Courts And Intellectual Property Subcommittee, 106th Cong. (1999) (Prepared Testimony of Ira Rubinstein, Senior Corporate Attorney, Microsoft Corporation, on Behalf of the Business Software Alliance).

See The Encryption Genie is Out of the Bottle, BUSINESS SOFTWARE ALLIANCE (visited March 8, 1999) <http://www.bsa.org/policy/encryption/index.html>.

See Kenneth Cukier, *U.S. Crypto Firms Develop Overseas*, COMMUNICATIONSWEEK INTERNATIONAL, March 24, 1997, at 18. California-based Pretty Good Privacy Inc., for example, struck such licensing agreements with European software developers. *See id.*

See Joint Statement: American Civil Liberties Union, Electronic Frontier Foundation, Electronic Privacy Information Center, ELECTRONIC PRIVACY INFORMATION CENTER, March 4, 1998 <http://www.epic.org/crypto/legislation/joint_statement_3_98.html>.

See Carol M. Ellision, *Who Owns Cryptography?, in* THE ELECTRONIC PRIVACY PAPERS 264, 271 (Bruce Schneier & David Banisar, ed., 1997)

See Niall McKay, *Teen Devises New Crypto Cipher*, WIRED.COM (Jan. 14, 1999) <http://www.wired.com/news/print_version/technology/story/17330.html?wnpg=all>. Ms. Flannery and her colleagues did, however, eventually break

advocates stress that there is no practical way to keep encryption within or without the confines of physical borders. For instance, anyone can easily purchase a copy of the encryption program Crypto II on the streets of Moscow for five dollars, and then e-mail it to a friend in New York.

Third, reform advocates argued that the government's treaty proposals would be ineffective even if states could control encryption within their borders. Specifically, they doubted that such a treaty could cover even a substantial potion of the over 1,600 encryption products available from more than 900 companies in 30 countries. Fourth, they pointed out that legal controls on encryption will bind only those who avail themselves to the law. Terrorists who are willing to blow up a building full of people will have no qualms about breaking laws against illegal encryption.

By 1999, advocates of encryption reform had placed considerable pressure on the government with legislation and legal challenges. The following is a short discussion of several of these efforts:

Legislation. Two important pieces of legislation squarely addressed the issue of encryption regulation.

SAFE. The most serious legislative challenge to the US encryption policy *statu s quo* was the "Security and Freedom through Encryption" (SAFE) Act, which was introduced by Representative Bob Goodlatte in 1999. SAFE would most

the cryptosystem she developed. *See Cryptography: An Investigation of a New Algorithm vs. the RSA*, available at <http://cryptome.org/flannery-cp.htm#ww>.

See John P. Barlow, Decrypting the Puzzle Palace, COMM. ACM, July 1992, at 25, 27.

See generally, e.g., Hearing of the House Judiciary Committee, Courts and Intellectual Property Subcommittee, 106th Cong. (1999) (prepared statement by Barbara A. McNamara, Deputy Director, National Security Agency); *The Security And Freedom Through Encryption (Safe) Act: Hearings on H.R. 850 Before the House Committee on The Judiciary Subcommittee on Courts and Intellectual Property*, 106th Cong. (1999) (prepared statement by Ronald D. Lee, Associate Deputy Attorney General).

See U.S. Technology Growth Being Undermined By Encryption Restrictions, SIIA Witness Tells House Judiciary Committee, SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (March 4, 1999) <http://www.siia.net/news/releases/ga/encrypt3499.htm>. The Software & Information Industry Association (SIIA) is the principal trade association of the software code and information content industry. The SIIA was formed on Jan. 1, 1999, as a result of a merger between the Software Publishers Association (SPA) and the Information Industry Association (IIA).

H.R. 850, 106th Cong. (1999).

basically guarantee all Americans the freedom to use any type of encryption anywhere in the world, and allow the sale of any type of encryption domestically. The Act would also specifically prohibit the federal government or the States from requiring key recovery or any other plaintext access capability in computer hardware or software. SAFE's greatest impact was, however, to come in the area of software exports. Indeed, the Act would require the Secretary of Commerce to grant export licenses for computer hardware or software if devices offering comparable security were commercially available outside the United States from a foreign supplier. In one of its few concessions to those weary of encryption, SAFE would set penalties for the unlawful use of encryption in furtherance of a criminal act—though it provided that the use of encryption would not be the sole basis for establishing probable cause.

Though previous incarnations of SAFE failed to win passage, in 1999 the measure enjoyed substantial support; 258 members of the House of Representative signed on as cosponsors. On July 21, 1999, however, the House Armed Services Committee voted to add language granting the President complete authority to deny any encryption exports he deemed "contrary to the national security interests of the United States." The House Intelligence Committee likewise adopted an "amendment in the nature of a substitute," which would continue most export controls. SAFE's fate thus rested in the hands of the House Rules Committee, which was to decide whether the pro-reform or *status quo* versions of the bill advanced to the House floor for a vote. Ultimately, however, the January 2000 changes preempted this choice; the bill's supporters have backed off, taking a "wait and see" approach regarding the administration's implementation of the changes.

PROTECT. Though the "Promote Reliable On-Line Transactions to Encourage Commerce and Trade" (PROTECT) Act called for more gradual change, its

The law make certain exception for encryption products for use by the Federal Government or a State, including investigative or law enforcement officers and members of the intelligence community.

"Probable cause" is the legal standard which allows law enforcement officers to search private property, or to make arrests.

SAFE was first introduced in 1995 as H.R. 3011, 103rd Cong. (1996).

See Bill Summary & Status for the 106th Congress-H.R.850, available at <http://thomas.loc.gov/cgi-bin/bdquery/z?d106:HR00850:@@@L>.

See id.

See Statement of Rep. Bob Goodlatte on Encryption Export Regulations, Jan. 13, 2000 (press release), available at <http://www.cdt.org/crypto/admin/000113goodlatte.shtml>.

S. 798, 106th Cong. (1999).

introduction was no less dramatic than that of SAFE. This is because PROTECT's sponsor, Senate Commerce Committee Chair John McCain, was until recently one of the strongest supporters of government key-recovery systems. Like SAFE, PROTECT would prohibit domestic controls on encryption products. On the export front, it would end the practice of conditioning export licenses on the inclusion of key recovery, and allow for the unfettered export of 64-bit cryptography. The Act would also establish a 12-member Encryption Export Advisory Board of national security officials and, significantly, representatives from private sector. PROTECT would, finally, authorize additional funding to assist law enforcement agencies in their quest to stay current with the latest security technologies. The Act did not, however, enjoy wide support, and was unlikely to reach the Senate floor for a vote.

Litigation. Three recent suits have challenged the legality of U.S. encryption export regulations: *Karn v. U.S. Dep't of State, Junger v. Daley,* and *Bernstein v. United States Dep't of Justice*. Though these cases all assert that the administrative procedures for reviewing encryption export applications are irrational, such claims stand little chance of success in light of the court's traditional and statutory deference to agency decision-making. The cases' stronger arguments, then, center on whether source code and encryption software warrant First Amendment freedom of speech protections.

Karn v. U.S. Dep't of State and *Junger v. Daley*. The *Karn* case centers on programmer Philip Karn's assertion that software code is speech, which should be able to publish freely. The codes Kern wishes to export are all readily available outside the U.S.

See Declan McCullagh, *McCain Offers Crypto Compromise*, WIRED. COM (Apr. 1, 1999) <http://www.wired.com/news/news/politics/story/18903.html>. Indeed, a bill Senator McCain introduced in the previous Congress would have retained strong encryption controls. *See* S. 909, 105th Cong. (1997).
925 F.Supp. 1 (D.D.C. 1996).
8 F. Supp. 2d 708 (N.D.Ohio 1998).
176 F.3d 1132,1999 U.S. App. LEXIS 8595 (9th Cir. 1999).
See 925 F.Supp. at 1.
For instance, the DES and 3DES algorithms is widely used all over the world. Enigma is a code used by the Nazis during World War II, and was cracked by the allies during than same period; finally, the IDEA algorithm was actually developed abroad and is available internationally as part of a software program called Pretty Good Privacy. *See Encryption Litigation*, CENTER FOR DEMOCRACY AND TECHNOLOGY (visited 5/11/99) <http://www.cdt.org/crypto/litigation/>.

Peter Junger is a law professor who sought to post the source code for his own encryption programs and standard commercial encryption software on a Web site for a computer law class at Case Western Reserve University Law School. When the Commerce Department deemed these postings illegal "exports," Junger filed suit in federal court on the theory that such a restriction violates his First Amendment free speech rights.

Both Karn and Junger suffered serious setbacks when their respective trial court judges dismissed the cases without trial (via summary judgment). Specifically, the court held that restriction on Karn's free speech rights were only incidental, and that the export regulations were justified because the government sought only "content neutral" control of the functional properties of the code. The *Junger* court similarly declared that though "exporting source code is conduct that can occasionally have communicative elements," "exporting software is typically non-expressive." Thus, U.S. restriction are not a prior restraint on speech because they do not impinge on "expression, or ... conduct commonly associated with expression." In essence, the judges agreed with the government's contention that encryption was more like the bombs on the munitions list than protected speech. Junger has

See 8 F. Supp. 2d at 713-14.

See id. at 711-12. Specifically, Junger's complaint alleged five such violations. "In Count One of his five-count complaint, Plaintiff Junger says licensing requirements for exporting encryption software work a prior restraint, violating the First Amendment's free speech clause. In Count Two, Junger argues that the Export Regulations are unconstitutionally overbroad and vague. In Count Three, he argues that the Export Regulations engage in unconstitutional content discrimination by subjecting certain types of encryption software to more stringent export regulations than other items. In Count Four, Junger claims that the Export Regulations restrict his ability to exchange software, by that infringing his First Amendment rights to academic freedom and freedom of association. In Count Five, Junger alleges that executive regulation of encryption software under the International Emergency Economic Powers Act, 50 U.S.C. § 1701 et seq., is a violation of the separation of powers doctrine." *See id.*

See 925 F.Supp. at 9. Karn then appealed the case to the Court of Appeals for the D.C. Circuit. By then, however, the Clinton administration had transferred jurisdiction over encryption exports from the State Department to the Commerce Department, and the D.C. Circuit sent the case back to District Court for a rehearing of the administrative law claim. *See* Karn v. U.S. Dep't of State, 107 F.3d 923 (D.C.Cir. 1997).

See id. at 717.

See id. at 718.

See id. (my emphasis).

appealed this ruling to the United States Court of Appeal for the Sixth Circuit, and Karn is likely to do the same .

Bernstein v. United States Department of Justice. Daniel Bernstein is a mathematician and cryptographer on the faculty of the University of Illinois at Chicago. Bernstien's suit centers on his efforts to export "Snuffle," an encryption program he wrote while a graduate student at UC Berkeley, along with its source code and an academic paper discussing the algorithm. After reviewing many of the procedural issues, the Court chose to focus on Bernstien's First Amendment claims.

In a clear contrast to the *Karn* and *Junger* rulings, Judge Patel of the Northern District of California held that encryption software is indeed protected expressive speech that cannot be stifled by the government's encryption export controls. On May 6, 1999, the Ninth Circuit Court of Appeals affirmed Judge Patel's ruling that the Export Administration Regulations (EAR) constituted a prior restraint on speech. According to the court, "insofar as the EAR regulations on encryption software were intended to slow the spread of secure encryption methods to foreign nations, the government is intentionally retarding the progress of the flourishing science of cryptography. To the extent the government's efforts are aimed at interdicting the flow of scientific ideas (whether expressed in source code or otherwise), as distinguished from encryption products, these efforts would appear to strike deep into the heartland of the First Amendment." However, the court emphasized the narrowness of its First Amendment holding by stating that not all software can be considered expressive. Though this decision represents a major challenge to the entire structure of government encryption regulation, the law is by no means settled; indeed, in January of 2000 the Ninth Circuit agreed to review the holding, and in May both Bernstein and the government requested that the appeals court remand the

A copy of Junger's appeal is available on the Internet at <http://samsara.LAW.CWRU.Edu/comp_law/jvd/pdj-brief.html >.

See 1999 U.S. App. LEXIS 8595 at 4.

See id.

See id. at 6-7 (citing Bernstein v. Department of State, 922 F. Supp. 1426 (N.D. Cal. 1996) ("Bernstein I"), Bernstein v. Department of State, 945 F. Supp. 1279 (N.D. Cal. 1996) ("Bernstein II"), and Bernstein v. Department of State, 974 F. Supp. 1288 (N.D. Cal. 1997) ("Bernstein III")).

Bernstein v. Department of State, 974 F. Supp. 1288 (N.D. Cal. 1997) ("Bernstein III").

See 1999 U.S. App. LEXIS 8595.

See id. at 35.

See Bernstein Crypto Case to be Reheard, ZD NET NEWS (January 27, 2000) <http://www.zdnet.com/zdnn/stories/news/0,4586,2428386,00.html>.

case back to the district court, so that the latter may assess the impact of the January 2000 policy changes to the case.

3 January 14, 2000 US Policy Reforms

On September 16, 1999 the Clinton administration announced that it recognized that "sensitive electronic information–government, commercial, and privacy information–requires strong protection from unauthorized and unlawful access." Thus, it pledged to institute new encryption regulations that would both "protect[] vital national security interests through an updated framework for encryption export controls . . . and . . . recognize[] growing demands in the global marketplace for strong encryption products."

3.1 New Regulations

The administration implemented these new policies in its January 14, 2000 revised regulations. Though these liberalize the encryption export regime, they retain government control of exports through three "principles": "a technical review of encryption products in advance of sale, a streamlined post-export reporting system and a process that permits the government to review exports of strong encryption to foreign governments." The following is a very general overview of the new regime:

Exports to Individuals and Commercial Firms. After a one time technical review, encryption products of any key length can be exported to any non-government end-user in any country (except for the seven "state supporters of terrorism"–Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria). This change subsumes the reforms of 1998, which covered subsidiaries, banks, financial institutions and other narrow industry sectors.

Retail Products. Using criteria such as functionality, sales volume, and distribution methods, the BXA will designate certain products as "Retail encryption commodities and software," which can be exported to any end user (except in the seven state supporters of terrorism). These products can

The respective requests are available at <www.eff.org/bernstein/20000303_bernstein_pr.html>.

See Administration Announces New Approach to Encryption, the White House Office of the Press Secretary, Sept. 16, 1999, available on the Internet at <http://www.bxa.doc.gov/Encryption/whpr99.htm>.

Id.

Revisions to Encryption Regulations, 65 Fed. Reg. 2492 (2000) (to be codified at 15 C.F.R. Pt.s 734, 740, 742, 770, 772, and 774) (proposed Jan. 14, 2000).

then be exported and reexported freely. According to the BXA, "finance-specific, 56-bit non-mass market products with a key exchange greater than 512 bits and up to 1024 bits, network-based applications and other products which are functionally equivalent to retail products are considered retail products."

Internet and Telecommunications Service Providers. The regulations provide a licence exception–meaning no technical review is required–to telecommunications and Internet service providers so that they may provide encryption services for the general public. They must, however, still obtain a license when providing such services for foreign governments.

"Open Source" Source Code. The January changes lift nearly all restrictions on open source code. The exporter must, however, submit to the Bureau of Export Administration a copy of the source code, or a written notification of its Internet location, by the time of export. It remains illegal, however, to "knowingly" offer such code to Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria.

Commercial Encryption Source Code and Toolkits. The regulations have also created a license exception for publically available commercial source code–*i.e.*, source code subject licensing or royalty fees. Again, no technical review is required, but the exporter must submit to the BXA a copy of the source code, or a written notification of its Internet address. All other source code can be exported only after a technical review to any non-government end-user.

U.S. Subsidiaries. Any encryption item of any key length may be exported or reexported to foreign subsidiaries of U.S. firms without a technical review.

Foreign Nationals. Foreign nationals working in the United States no longer need an export license to work for U.S. firms on encryption.

Export Reporting. Though many products can now be exported even without a technical review, many post-export reporting requirements remain. No such reporting is required, however, for finance-specific or retail product exports to individual consumers. Additionally, no reporting is required if the product is exported via free or anonymous download, or is exported from a U.S. bank, financial institution or their subsidiaries, affiliates, customers or contractors for banking or financial use.

3.2 Impact of the January 14, 2000 US Policy Reforms

The January regulations represent a dramatic liberalization of US encryption policy. Nonetheless, questions remain as to the implementation of these

regulations. Specifically, many exports still require "technical reviews," wherein exporters must present their products for BXA approval. At this point in the process, the BXA maintains broad authority to prevent export of the product. There are also questions as to the speed and diligence with which the BXA will implement the technical reviews.

The provision covering the "knowing" export of encryption products to a person from Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria country also raises practical questions. Under this provision, for instance, it would be illegal to post source code to a newsgroup if the poster knows that the forum also hosts Iranian visitors.

Note finally that, while the *Bernstein* plaintiffs have expressed some satisfaction at the new policies, they vowed to continue their case, hoping that their First Amendment arguments will undercut the very foundation for the government's authority to regulate encryption in the first place.

4 Israel's Security and Economic Concerns

Before examining Israel's encryption policy, it is important to briefly review the context in which it evolved. Indeed, much like the United States, Israel must weigh both security and economic concerns when formulating an encryption policy.

4.1 National Security Concerns

Israel's history has been one of simmering conflict punctuated war in each of the five decades since it was established. Both its leaders and population perceive that these conflicts threaten not only the nation's borders, but also its very existence. Israel's citizens also live under the constant threat of terrorist attack; in February and March of 1996, for instance, Islamic militants seeking to undermine the Middle East peace process blew up 65 people on public busses in Tel Aviv and Jerusalem. Less spectacular attacks like

See MENACHEM HOFNUNG, DEMOCRACY, LAW, AND NATIONAL SECURITY IN ISRAEL 2 (1996).

See B. KIMMERLING, THE INTERRUPTED SYSTEM: ISRAELI CIVILIANS IN WAR AND ROUTINE TIMES, 5-6 (1985).

See UNITES STATES STATE DEPARTMENT, PATTERNS OF GLOBAL TERRORISM (1996), available at <http://www.state.gov/www/global/terrorism/1996Report/middle.html>.

politically motivated stabbings take place regularly. In this context, national and individual security has become the top priority of Israel's leaders.

Though Israel tightly controls intelligence information, the army has confirmed that Hamas and other Islamic militants regularly use the Internet to transmit encrypted instructions for terrorist attacks—"including maps, photographs, directions, codes and even technical details of how to use bombs." Army officials believe that militant cells in the West Bank receive this information from the United Kingdom, Damascus and Khartoum. Specifically, militants use publicly available encryption applications originally developed to secure credit card information traveling across the Web.

4.2 Economic Considerations

Over the last decade Israel has transformed its economy from one based on agriculture, commerce and light industry, to one which increasingly relies on high technology—sectors like communications, electronics, information technology, biochemistry and agritechology.

These high-value added industries have brought tremendous economic growth; from 1990 to1996, for instance, Israel's gross domestic product expanded at approximately 6% a year, catapulting the country's standard of living well into the range of Western Europe's. Currently, over 27% of the work force is employed in technical professions, as compared to 8% in the US or 12% in Japan. Israel's prominence in these emerging high

See, e.g., UNITES STATES STATE DEPARTMENT, PATTERNS OF GLOBAL TERRORISM (1997), available at <http://www.state.gov/www/global/terrorism/1997Report/mideast.html>.

See generally, HOFNUNG, *supra* note 66 at 2.

See Julian Borger, *Hamas Accused of Using Internet as Terror Tool*, THE GUARDIAN (LONDON), Sep. 27, 1997, at 17 (citing investigators from the Israeli civilian intelligence organization, the Shin Bet).

See id.

See id.

See ISRAELI MINISTRY OF FINANCE, THE ISRAELI ECONOMY: AN OVERVIEW (visited March 19, 1999) <http://www.mof.gov.il/englishframe.htm>; *see also* STANDARD AND POOR'S, ISRAEL: BASIC INFORMATION (visited Mar. 18, 1999) <http://www.standardpoor.co.il/economy-index.html>.

See MINISTRY OF FINANCE, *supra* note 74. In 1997, Israel's Gross Domestic Product per capita fell just behind the United Kingdom but ahead of Ireland and Spain. *See id.*

See id.

technology fields has led many to dub it the "second Silicon Valley," or, alternately, the "Silicon Wadi."

As Israel is small—about 5.6 million people living in an area the size of New Jersey —much of this economic productivity is directed outwards. The Israeli Manufacturers' Association reports that in 1999 software exports totaled $2 billion dollars, a 33% increase over 1998 (which itself saw a 50% increase over 1997). Israel must also raise capital abroad, and indeed in 1998 U.S. stock markets listed over 100 Israeli companies, nearly all of which focus on high technology. Finally, Israel gains revenue from the investments of top U.S. technology corporations such as Microsoft, Intel, IBM and Motorola, all of which maintain research and development centers in the country.

This economic reliance on technology exports is largely a matter of necessity. Though it supports an extensive agriculture sector, Israel is essentially a nation of limited natural resources. Its competitive advantage is rather in the skills of its people; Israel has more scientists and engineers per capita than any other nation, with 135 for every 10,000 citizens. These

See STANDARD AND POOR'S, *supra* note 74; *see also The Hot New Tech Cities*, NEWSWEEK, November 3, 1998.

See, e.g., Mark Simon, *Greetings from Siliconia,* SAN FRANCISCO CHRONICLE, Sept. 24, 1998, at A19; *see also* Rebecca Trounson, *Ancient Land Looks to a Cutting-Edge Future*, LOS ANGELES TIMES, April 12, 1998, at S3.

See UNITED STATES CENTRAL INTELLIGENCE AGENCY, ISRAEL, THE WORLD FACTBOOK-1998 (1998) [hereinafter CIA FACTBOOK], found at <http://www.odci.gov/cia/publications/factbook/is.html>.

See MINISTRY OF FINANCE, *supra* note 74. Israel's economy is generally reliant on international trade; exports plus imports in goods and services amount to over 80% of GDP. *See id.*

See Keren Tsuriel, *'99 Software Exports Up 33% to $2 Bln,* GLOBES (Jan. 25, 2000) <http://www.globes.co.il/cgi-bin/Serve_Archive_Arena/pages/English/1.3.1.1/20000124/2>; Ella Jacoby, *Israel's Software Exports Up 50% in '98*, GLOBES (Feb. 2, 1999) <http://www.globes.co.il/cgi-bin/Serve_Archive_Arena/pages/English/1.2.1.17/19990201/1>.

See TROUNSON, supra note 78.

See id. Intel is building a $ 1.6-billion semiconductor plant near Tel Aviv.

See id.

See CIA FACTBOOK, *supra* note 79.

See TROUNSON, *supra* note 78. There are 85 scientists and engineers for every 10,000 U.S. citizens. *See id.* Over 30 percent of Israel's work force boasts 13 or more years of education, and 26 percent hold academic degrees in the sciences. *See* Felix Zandman, *Business, Despite The Terror*, JOURNAL OF COMMERCE, May 31, 1996, at 7A.

numbers were reinforced by this decade's massive influx of technically skilled immigrants from the former Soviet Union—a number expected to reach around 1,000,000 by the year 2000.

Finally, it is important to note that, rather than serving as an obstacle to commercial encryption development, the Israeli military has been crucial to the sector's growth. Indeed, many of Israel's technology entrepreneurs developed their skills and professional networks while conducting advanced research in military labs. Israeli army veterans have especially excelled in establishing companies which focus on software security, of which encryption is a vital component. One such company is Check Point Software Technologies Ltd., a network security and management firm. Founded in 1993, the Israeli-based corporation and its United States subsidiary quickly grew to command a large portion of the global market for firewall systems which protect corporate computer networks from intruders. Check Point's sales totaled $219 million in 1999.

5 Israel's Encryption Policy

See MINISTRY OF FINANCE, *supra* note *74.* One third of these ex-Soviet Jews possessed both technical education and skills. *See* ZANDMAN, *supra* note 85. *See, e.g., How Israeli High-Tech Happened*, GLOBES (visited Mar 28, 1999) <http://www.globes.co.il/cgi-bin/Serve_Arena/pages/English/1.2.2.1.1.2>; *see also* TROUNSON, *supra* note 87.

See, e.g., John Rossant, *Out of The Desert, Into the Future*, BUSINESS WEEK, Aug. 21, 1995, at 78; *see also* TROUNSON, *supra* note 78.
Gil Shwed, President, CEO and co-founder of Checkpoint served in a computer programming unit of the Israeli Defense Forces. *See Gil Shwed (profile)*, CHECK POINT SOFTWARE TECHNOLOGIES LTD. (visited March 28, 1999) <http://www.checkpoint.com/corporate/gilshwed.html>. E-mail security firm Vanguard Security Technology's Chief Technology Officer Raviv Karnieli is likewise a product of a software engineering unit at the Israeli Air Force. *See About Us,* VANGUARD SECURITY TECHNOLOGY (visited march 28, 1999) <http://www.vguard.com/about.html>.
See Corporate Profile, CHECK POINT SOFTWARE TECHNOLOGIES LTD. (January, 1999) <http://www.checkpoint.com/corporate/corporate.html>.
See id.
See Check Point Software Technologies Ltd. Reports Another Record Fiscal Year, CHECK POINT SOFTWARE TECHNOLOGIES LTD. (Jan. 18, 2000) <http://www.checkpoint.com/press/2000/q499earnings011800.html>.

Paying special attention to important 1998 Amendments, this section will briefly review the laws and regulations which control Israeli encryption policy. It will then discuss how the government has implemented these regulations.

5.1 Laws and Regulations

The government's underlying authority to regulate encryption is found in the Law for Control of Products and Services of 1957 (the "Control Law"). This law grants Israeli Ministers broad powers to regulate by declaration the production, export, distribution, and sale of products. Though these powers are nominally limited to periods of a formal "state of emergency," such a state has in fact existed uninterrupted since it was proclaimed by the Provisional Council of State at the nation's founding in 1948.

Encryption development fell into the sphere of the Control Law following the disastrous intelligence failures of the 1973 Yom Kippur War. Specifically, the Minister of Defense promulgated the Control of Products and Services Declaration (Engagement in Encryption) of 1974 (the "Encryption Declaration"), which states that "engagement in means of encryption . . . is a service under control" for purposes of the Control Law. A 1998

See Ori Rosen, *Israel: Cryptography Law and Policy, in* Stewart A. Baker and Paul R. Hurst, THE LIMITS OF TRUST 175, 176 (1998) (citing *Sefer Hukim*, 5718, at page 24).

See id. Israeli law uses the terms declaration interchangeably with regulations, rules, and orders. *See id.* at fn. 2.

See id. at 176.

See HOFNUNG, *supra* note 66, at 49. For an interesting discussion of the impact of this "noramalization" of emergency legislation, *see id.* at 47-70. It is interesting to note that the Israeli Supreme Court's has commented that this arrangement is inconsistent with the principle of the rule of law. *See* Rosen, supra note 93, at 176 (citing HCJ 156/63 The General Attorney v. Ostreicher, 17(3) Piskey Din 2088; HCJ 266/68 Petach Tikva Municipality v. The Minister of Agriculture, 22(2) Piskey Din 824; HCJ 790/78 Rosen v. The Minister of Trade and Tourism, 33(3) Piskey Din 281).

In November of 1999, however, the Israeli cabinet announced that it plans to end the state of emergency. *See Sari Bashi, Israel Takes Step Toward Abolishing 51-year Old State of Emergency*, ASSOCIATED PRESS, Nov. 21, 1999. According to the cabinet, some emergency measures would be adopted in the form of specific laws, and some will be abolished. *See id.*

See Kovetz Takanot, 5735-1975, at page 46. The Hebrew text of this law is also available on the Internet at <http://www.law.co.il/computer-law/main.htm>.

Id. at § 2(a).

amendment has updated the definition of "Encryption means" to read "the development, manufacture, modification, integration, purchase, use, keeping, transfer from place to place or from hand to hand, import, distribution, sale or conduct of export negotiations or export of means of encryption."

The Minister of Defense then issued encryption regulations, in the form of the Control of Commodities and Services Order (Engagement in Means of Encryption) of 1974 ("the Encryption Order"), which was itself amended by the Control of Commodities and Services Order (Engagement in Means of Encryption) of 1998 (Amendment). The Encryption Order requires that anyone "engaged in means of encryption" receive a license from the Director-General of the Ministry of Defense. At his discretion, the Director-General may grant a "general license," which is an open-ended license for nearly all types of engagement in encryption means; a "limited license" which is limited by types of permissible encryption, destination countries, or other criteria; or a "special license," which is limited to a certain transaction of certain encryption means. According to the 1998 revisions, the Director-General may also deem certain encryption technology to be "free means," for which all license requirements are waived.

To date, the Ministry of Defense has published neither information regarding the criteria for the review of license applications, nor a timetable for the processing of these documents. There are also no reported court cases on this process. The 1998 amendment did, however, establish an Advisory Committee to assist the Director-General in "exercising his powers

The Commodities and Services Declaration (Engagement in Means of Encryption) of 1998(Amendment) [hereinafter 1998 Encryption Declaration], available at HAIM RAVIA: LAW OFFICES (visited March 28, 1999) <http://www.law.co.il/computer-law/main.htm>.

See Kovetz Takanot, 5735-1975, [hereinafter 1975 ENCRYPTION ORDER] at page 45. The Hebrew text of this law is also available on the Internet at <http://www.law.co.il/computer-law/main.htm>.

[Hereinafter 1998 ENCRYPTION ORDER], vailable at HAIM RAVIA: LAW OFFICES (visited March 28, 1999) <http://www.law.co.il/computer-law/main.htm>.

See id. at § 2. Until the 1998 revision this responsibility rested with the Israeli Defense Force's Chief Communications and Electronics Command ("CCEC"). *See* 1975 ENCRYPTION ORDER, *supra* note 100.

See 1998 ENCRYPTION ORDER, at §§ 1,2.

See id.

See id.

See 1998 ENCRYPTION ORDER, at § 3B.

See ROSEN, *supra* note 93, at 183.

See id, at 183.

See ROSEN, *supra* note 93, at 183-184.

under [the] Order." The fact that the regulations call for civilian participation in this committee may reflect a desire to give greater consideration to business and other civilian interests.

The Department of Defense retains broad discretion over encryption even after it grants a license. Specifically, officers of the Ministry may at any time enter any place where the licensee engages in encryption means, examine the means, and require the applicant to provide pertinent records and information in connection with the means. The Director-General may also suspend or revoke the license at his discretion. The law finally bars the licensee from disclosing information about encryption to anyone but the people listed on the license or those which the Director-General later approves.

5.2 Application of the Israeli Regulations

The 1998 revisions came as a response to growing criticism of Israel's draconian encryption policies. In a 1997 essay on the topic, Israeli lawyer Ori Rosen described the "red-tape journey" of a company wishing to develop software that contains encryption. As with the present system, the company required a permit before developing its product—though at that time the licensing body was within the Israeli Defense Forces. If granted, however, the permit was only good for a year, and would need to be reissued if the product was revised. The company would need another one-year license to sell the product domestically, and yet another from the Ministry of Defense if it wished to sell the product abroad. To make matters worse, Rosen reported that the application process often took months.

Criticism of this system came from within the government as well. In the Summer of 1997, a committee of experts working with the Israeli National Committee for the Development of Information and Communication Infrastructure ("Expert Committee") issued a report critical of the status quo. The report called the law's broad definitions "absurd," and found that they unreasonably restricted the ability of Israeli companies to compete on

See 1998 ENCRYPTION ORDER, at § 10A.

See 1975 ENCRYPTION ORDER at § 2(b) and modifications in 1998 ENCRYPTION ORDER, at §§ 1,2.

See id.

See id. at § 2(b).

See id. at § 8.

See ROSEN, *supra* note 93, at 182-183.

This report may be found at the Knesset Web site, at <http://www.knesset.gov.il>.

the world market. The report also echoed many of the criticisms outlined in the previous sections, specifically questioning the assumption that export controls can help protect the national security:

> The basic argument, which may have had some weight at the time the [Encryption] Order was issued, in 1974, was that the regulation of encryption technologies, in general, and the prohibition on the use of "strong" encryption means in particular, will keep these technologies off the hands of those in whose communications the security authorities are interested. Needless to say, the validity of this argument today has been seriously weakened, when encryption technologies are available with minimal effort to all. Hence, the Encryption Order is being enforced only on law abiding citizens.

In light of these findings, the fact that Israeli companies like Checkpoint prospered even under the pre-1998 Encryption Order suggests that the security establishment enforced the law flexibly. Indeed, an examination of pre-1998 product announcements reveals that Israeli companies were exporting strong encryption even during that period, and testimony about encryption in the US Congress rarely failed to mention Israel's status as an aggressive encryption developer and exporter. Further, in discussing encryption with Israeli software engineers, the author of this article found that many were unaware of the regulations' specifics, and had been developing software and conducting research with no interference from the government for years. Such an enforcement approach suggests a recognition of the difficulty of controlling encryption, a recognition of the economic importance of a competitive high-technology industry, or even to the fact that many of these companies are headed by veterans of army technical units and therefore "trustworthy."

See id.

Id. The English translation for the paragraph comes from ROSEN, *supra* note 93, at 185.

See, e.g., Vanguard Launches Mail Guardian Encryption Software, NEWSBYTES, February 2, 1998 (announcing Israel-based Vanguard Security Technologies' shipment of its "Mail Guardian" product, which adds 56-bit DES encryption to popular Internet e-mail packages); *see also Check Point & 3Com Corporation Announce Enterprise Security Technology Agreement*, M2 PRESSWIRE, March 25, 1997.

See, e.g., Online Encryption Technology: Hearing of the Senate Commerce, Science and Transportation Committee, 104th Cong. (1999) (statement of James Barksdale, Chief Executive Officer of Netscape Communications).

See supra text accompanying Section 4.

In this context, the Amended Encryption Order of 1998 may have been an attempt to bring encryption regulations into conformity with the prevailing enforcement practices, especially as number of companies producing encryption products has grown beyond the number manageable by personal relationships. Most notable is the consolidation of the license process into one office which may issue the general, open-ended license. The authority to altogether "free" an encryption means from the licensing procedures is also an innovation, especially if it will be used to implement the Expert Committee's recommendation that the state refrain from "limit[ing] the use of means that can be freely obtained from many public sources." Finally, the new civilian input via the Advisory Committee may help influence the Ministry of Defense to give greater weight to commercial and privacy views when licensing encryption. Essentially, the 1998 Amendment create a licensing system which at least potentially allows Israeli companies to develop and "export competitive products that can be marketed in most of the world's countries as off-the-shelf products."

Though the 1998 Amendments are a marked improvement of Israel's policy, several problems remain. First, the Director-General retains nearly complete discretion in issuing licenses, as there are no written guidelines. Even the Expert Committee's report is not a comprehensive guide; it does not, for instance, address how Israel should balance the government's interest in keeping cutting edge-cryptography secret for its own use against the interest of Israeli companies in introducing products that are not widely available and therefore highly marketable. The requirements for a permit even to negotiate a sale of encryption are likewise impractical in today's competitive business environment. Other critics point out that, applied literally, the law is still overbroad, as any Israeli using a Web user is technically "using" means of encryption every time he or she makes a secure connection to, for instance, transmit credit card data.

As with their predecessors, the test of the 1998 Amendments' impact rests in their application. As the Ministry of Defense releases virtually no information on the program, such progress is difficult to evaluate. It seems, however, that at they least have not tightened controls; since the 1998 Amendments Checkpoint, Algorithmic Research, Radguard, and Aliroo have continued to aggressively develop and export strong encryption.

See EXPERT REPORT, *supra* note 116.

Id.

Israeli attorney Haim Ravia makes this argument in *The New Code Order*, HAIM RAVIA: LAW OFFICES (visited March 30, 1999) <http://www.law.co.il/articles.htm>.

See Check Point Software Technologies Offers New Strong Encryption IPSec Solutions in The United Kingdom, CHECK POINT SOFTWARE TECHNOLOGIES LTD. (Nov. 17, 1998)

6 Conclusion

After years of glacial reform, the rapid and dramatic liberalization of encryption policy in Israel and the US reflects a growing acknowledgment that encryption is too difficult to control and too valuable to suppress. Though there are some notable counter- examples, the market forces which demand strong data privacy are likely to accelerate this evolution by forcing countries to permit the commercial exploitation of ever more powerful encryption.

<http://www.checkpoint.com/press/1998/ipsec111798.html> (announcing plans to ship products using the 156-bit Triple DES encryption technology to the United Kingdom).

See Security Products, ALGORITHMIC RESEARCH (visited March 28, 1999) <http://www.arx.com/html/products/cryptoserver.html> (describing development and export of cryptographic data security products with keys as large as 2048-bits).

See Products, RADGUARD (visited March 25, 1999) <http://www.radguard.com/products.html>. Radguard is a leading producer of Network Security products.

See Aliroo Signs Agreement to Add RSA Encryption to PrivaWall, PrivaSuite and PrivaSeal, ALIROO, INC., (January 20, 1999) (describing products containing strong encryption—including Triple DES—for the protection of privacy in email documents, Internet file transfer, Groupware, faxes and archiving).