Northwestern Journal of Technology and Intellectual Property

Volume 11 | Issue 7 Article 5

Fall 2013

International Cryptography Regulation and the Global Information Economy

Nathan Saper

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

International Cryptography Regulation and the Global Information Economy

Nathan Saper

September 2013 VOL. 11, NO. 7

Northwestern Journal of Technology and Intellectual Property
Volume 11, Number 7 (September 2013)

International Cryptography Regulation and the Global Information Economy

By Nathan Saper*

I. INTRODUCTION

¶1 As information technology products and services begin to account for larger shares of international trade, and as companies engaging in foreign direct investment begin to focus more on high-technology areas with attendant risks to intellectual property, the importance of information security will continue to grow. A key component of any robust information security system is cryptography. Cryptography allows for the protection of sensitive information, either in storage or in communication, and is a necessary feature of any secure e-commerce or electronic communication system (including secure email and voice communication). In the United States, there are few restrictions on the use of cryptography. When operating overseas, however, companies must grapple with a bewildering array of regulations and restrictions on the use of cryptography. Some countries restrict the import or export of cryptographic technology, others restrict the import of encrypted data, and still others restrict or prohibit the use of

* J.D., 2013, Northwestern University School of Law.

encryption within their borders. These regulations create immense difficulties for firms attempting to operate overseas, especially where prohibitions on the use of encryption force them to put their intellectual property at risk of compromise. Furthermore, the United States places restrictions on the export of encryption technology, and these restrictions can place companies operating overseas at risk of severe penalties if cryptography systems are exported to prohibited countries or entities.

¶2 With the meteoric rise of the Internet and e-commerce in the 1990s came great attention to the problems and opportunities associated with cryptography. Throughout that decade, the United States and many foreign countries debated and experimented with various forms of cryptography regulation, and attempts were made at international harmonization. Since then, however, policy-making activity around cryptography has slowed, if not halted altogether, leaving individuals and companies to face a bewildering array of regulations—or, in many cases, to face regulations that are extraordinarily unclear and haphazardly applied.

¶3 This Note seeks to introduce the reader to the issue of international cryptography regulation by focusing on laws in a select group of countries, including the two largest global economies—China and the United States. Section II of this Comment provides a brief introduction to cryptography and its applications. Section III provides an overview of cryptography regulation generally—including its rationale and history—and in a selection of important markets. In Section IV, this Comment discusses the impacts of the current global patchwork of encryption regulation on businesses and individuals. Finally, Section V of this Comment proposes security best practices for organizations operating internationally.

II. INTRODUCTION TO ENCRYPTION AND CRYPTOGRAPHY

¶4 Encryption is the primary tool that allows for information security in the digital age. In its most basic form, encryption takes a message or document and scrambles it so that only intended recipients can view the contents.[1] An unencrypted document—for example, an email message—can be viewed and understood by anyone who receives it; an encrypted document, on the other hand, cannot be read or viewed by unintended recipients, even if they have possession of the document itself.

¶5 Encryption works by taking an original, unsecured document—called the *cleartext*—and using a key to transform it into a secured document—the *ciphertext*.[2] Cryptography is not new; in fact, encryption in simple forms has been in use for thousands of years. The Roman emperor Julius Caesar employed an encryption method based on a very simple key: in his communications, he would shift each letter in the alphabet up by three letters.[3] The science of cryptography has advanced considerably

[1] Tricia E. Black, Note, *Taking Account of the World As It Will Be: The Shifting Course of U.S. Encryption Policy*, 53 FED. COMM. L.J. 289, 292 (2001).

[2] D. RICHARD KUHN ET AL., NAT'L INST. OF STANDARDS & TECH., *INTRODUCTION TO PUBLIC KEY TECHNOLOGY AND THE FEDERAL PKI INFRASTRUCTURE 9* (2001), *available at* http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf.

[3] Nicholas J. Patterson, *The Key Theory: Authenticating Decrypted Information in Litigation While Protecting Sensitive Sources and Methods*, 88 TEX. L. REV. 1767, 1769 (2010).

since the time of Caesar, however, and modern encryption methods in widespread use today involve complicated mathematical algorithms.[4]

¶6 There are two basic types of encryption in contemporary use: symmetric (or "private") key systems and asymmetric (or "public") key systems. Symmetric key systems are the simpler of the two. In a symmetric system, the same key is used to both encrypt and decrypt the document.[5] A common example of this form of encryption is the password protection function of word processors, such as Microsoft Word, by which a user can lock a document with a password, and then if she sends the document to a colleague, the colleague will need to use the same password to open the document. This form of encryption is sufficient for protection of personal documents, where a user wants to prevent everyone but herself from accessing her files. However, symmetric encryption is problematic when one wants to securely communicate with others, because, before the secure communication can be initiated, the participants must first agree on a key (or in the word processor example above, a password). While agreeing on a key in advance may be easy in an office setting where all participants can communicate face-to-face, this is impossible in many common situations. If the communicating parties are not in the same room, symmetric cryptography creates a chicken-and-the-egg problem: before the parties can communicate securely, they must first exchange a key, and this exchange must occur over an insecure channel, thereby breaking the security of the communication before the encryption has even occurred.[6]

¶7 The key-exchange problem was solved in the 1970s with the advent of asymmetric key systems.[7] Whereas in a symmetric key system the same key is used for both encryption and decryption, in an asymmetric key system, one key—the *public key*—is used for encryption, and a separate key—the *private key*—is used for decryption.[8] The public key and the private key are mathematically related;[9] the breakthrough that led to the development of asymmetric cryptography was the discovery of mathematical arrangements that make it nearly impossible to derive the private key from a user's public key.[10] A user's public key can be made generally available (e.g., by posting on her website), and anyone who wants to send an encrypted document to the user can download her public key and use it to encrypt the message. However, the message cannot then be decrypted by anyone—including the original sender of the message—unless they have the user's private key, and this key the user keeps secure.[11]

¶8 Asymmetric cryptography opened entirely new uses for encryption and facilitated the development of many aspects of modern life that we now take for granted. The ability to initiate a secure communications channel between two parties who had never before communicated—and who could be complete strangers, and even anonymous—

---

[4] Black, *supra* note 1, at 294–95.
[5] *Id*. at 296.
[6] *See* D. RICHARD KUHN ET AL., NAT'L INST. OF STANDARDS & TECH., INTRODUCTION TO PUBLIC KEY TECHNOLOGY AND THE FEDERAL PKI INFRASTRUCTURE 10 (2001), *available at* http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf.
[7] Greg Vetter, *Patenting Cryptographic Technology*, 84 CHI.-KENT L. REV. 757, 761-62 (2010).
[8] *Id.* at 11.
[9] *Id*. at 11, 49.
[10] Greg Vetter, *Patenting Cryptographic Technology*, 84 CHI.-KENT L. REV. 757, 762 (2010).
[11] Black, *supra* note 1, at 296.

made possible the growth of all forms of e-commerce on the Internet.[12] Asymmetric cryptography underlies Hypertext Transfer Protocol–Secure (HTTPS), which is the protocol that allows for secure communication between servers and clients on the World Wide Web.[13] Without asymmetric cryptography, it would be impossible for users of the Internet to communicate securely with e-commerce vendors, online banking websites, and the like.

¶9 The encryption systems in use today can be made extraordinarily secure. The strength of an encryption system is determined by three factors: key security, the security of the underlying algorithm, and key length.[14] Key security is the responsibility of users, and hence is usually the least secure component of a cryptography system.[15] Assuming that users safeguard their keys, however, modern cryptography systems are very secure. The algorithms they use have been extensively researched and tested to ensure mathematical security, and the keys used are long enough to make a brute-force attack impractical.[16] Popular and widely-available encryption software, using tested algorithms and sufficiently long keys, can make data virtually impenetrable to attack.[17]

¶10 Because data that have been encrypted with a strong cryptography system cannot be retrieved without the decryption key, managing those keys is a matter of great importance for organizations. This is particularly important in the case of asymmetric cryptography, where a single public-private key pair may be used for innumerable communications and transactions; if the private key is lost, all prior communications become inaccessible, and the key pair itself becomes unusable. To manage this risk, the concept of key escrow was developed.[18] With key escrow, a copy of each decryption key is placed in escrow with a trusted third party (TTP); if the key holder loses her copy of the key, the TTP can recover it.[19]

¶11 Many large organizations operate their own key escrow systems. A more important example of a key escrow system, however, is the case of certificate authorities (CAs). Certificate authorities are organizations (either private companies or governmental agencies) that issue public-private key pairs to authenticated organizations or individuals.[20] For example, if an individual wants to start an e-commerce website that uses encryption and is trusted by consumer web browsers, that individual can request that a certificate authority issue a key pair in her name. The certificate authority will verify that the person requesting the certificate is who she claims to be (by, for example,

---

[12] *See id*. at 294.

[13] *See* T. Dierks & E. Rescorla, *The Transport Layer Security (TLS) Protocol, Version 1.2*, NETWORK WORKING GROUP (Aug. 2008), http://tools.ietf.org/html/rfc5246.

[14] Aaron Perkins, Comment, *Encryption Use: Law and Anarchy on the Digital Frontier*, 41 HOUS. L. REV. 1625, 1628 (2005).

[15] Key security can be compromised by, for example, users writing their passwords on notecards on their desks.

[16] Perkins, *supra* note 14, at 1628-29. A brute-force attack is an attempt to break encryption by trying all possible decryption keys. As the key in use is lengthened, the number of possible keys increases exponentially, and the system becomes less vulnerable to brute-force attack. D. Forest Wolfe, Comment, *The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption*, 49 EMORY L.J. 711, 716 (2000).

[17] Patterson, *supra* note 3, at 1769–70.

[18] *See* HAL ABELSON ET AL., THE RISKS OF KEY RECOVERY, KEY ESCROW, AND TRUSTED THIRD-PARTY ENCRYPTION 6 (1997), *available at* http://www.schneier.com/paper-key-escrow.pdf.

[19] Wolfe, *supra* note 16, at 717.

[20] *See* Black, *supra* note 1, at 301.

requesting a copy of government-issued identification), and once the individual is authenticated, the CA will then issue a public-private key pair in her name.

¶12 Certificate authorities are a critical component of the architecture of the Internet. A relatively small number of certificate authorities are "trusted" by the major web browser vendors (such as Microsoft, Mozilla, Google, and Apple).[21] This means that web browsers from those vendors automatically assume the validity of encryption keys issued or verified by those certificate authorities. However, certificate authorities also represent a potential weakness in the security architecture of the Internet. Certificate authorities, like other trusted third parties, maintain copies of all private keys that they have issued, or that have been made available to them. This means that if a certificate authority is compromised, an enormous number of keys may be compromised. Furthermore, if the certificate authority is untrustworthy itself, it may use the decryption keys for unintended purposes.[22]

¶13 Today, nearly all participants in society use encryption. Governments and corporations use encryption to secure documents, emails, and voice communications.[23] Individuals use encryption—though they likely do not realize it—every time they use the Internet to purchase a book, engage in online banking, or otherwise conduct e-commerce.[24] Encryption makes it possible to submit credit card information and other sensitive data over the Internet without revealing the information to man-in-the-middle attacks and other vulnerabilities. Encryption also makes possible the creation and use of digital signatures, which allow for authentication on the Internet.[25] Finally, encryption makes it possible for organizations and individuals who wish to communicate without fear of government monitoring to do so—whether those individuals be human-rights advocates in authoritarian states, terrorists, or narcotics traffickers.

III. CRYPTOGRAPHY REGULATION AROUND THE WORLD

A. Cryptography Regulation, Generally

¶14 Most major countries regulate encryption, to varying degrees. Encryption is regulated because it is a "dual-use" technology; that is, it has both commercial and military value.[26] The United States pioneered the efforts to regulate encryption during the Cold War.[27] Since then, U.S. encryption regulation has been driven by two competing concerns: "(1) the ability of American high-tech industries to compete in foreign markets; and (2) the ability of criminals and terrorists to threaten national security

[21] For example, the Firefox web browser and other products from the Mozilla Foundation automatically trust certificates issued by over fifty companies. *Mozilla Included CA Certificates*, MOZILLA, http://www.mozilla.org/projects/security/certs/included/index.html (last modified June 10, 2013).

[22] This is of particular concern where governments themselves operate certificate authorities.

[23] *See* Patterson, *supra* note 3, at 1769–70.

[24] *Cf.* Black, *supra* note 1, at 292.

[25] Lyombe Eko & Natasha Tolstikova, *To Sign or Not to Sign on the Electronic Dotted Line: The United States, the Russian Federation, and International Electronic Signature Policy*, 10 INT'L J. COMM. L. & POL'Y 1, 2 (2005), *available at* http://ijclp.net/old_website/10_2005/pdf/ijclp_05_10_2005.pdf.

[26] Aimee Boram Yang, Note, *China in Global Trade: Proposed Data Protection Law and Encryption Standard Dispute*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 897, 909-10 (2008).

[27] *See* Christopher F. Corr, *The Wall Still Stands! Complying with Export Controls on Technology Transfers in the Post-Cold War, Post-9/11 Era*, 25 HOUS. J. INT'L L. 441, 450-52 (2003).

through the use of strong encryption."[28] However, other countries' encryption regulations may be meant to serve other ends, e.g. the monitoring and restriction of domestic speech. This regulatory patchwork creates substantial challenges and risks to firms operating internationally.

¶15 In an effort to harmonize regulations on the export and import of dual-use technologies, many countries have come together and agreed to a set of principles known as the Wassenaar Arrangement.[29] The stated goal of the Wassenaar Arrangement was "to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies . . . ."[30] Cryptography is classified as a dual-use good.[31] The Wassenaar Arrangement makes symmetric cryptography products of up to 56 bit key length, and asymmetric cryptography products of up to 512 bit key length, free from export restriction.[32] Furthermore, the Wassenaar Arrangement includes a personal-use exemption, allowing individuals who travel abroad to carry with them cryptography devices for their personal use.[33] However, cryptography products that do not fall into these exemptions are still eligible for restriction.[34] The Wassenaar Arrangement sets general parameters for import and export control to which member states largely adhere; however, the Wassenaar controls are not binding on member states and are implemented at the discretion of member governments.[35]

B. Cryptography Regulation in the United States

¶16 The United States, in addition to being the current primary producer of information-technology and security products today, also has among the most well-developed and documented laws regarding encryption. Hence, American encryption regulation is a useful place to begin an inquiry into the global framework of encryption regulation. The United States does not place any restriction on the domestic use, creation, or sale of encryption products domestically.[36] Furthermore, there is no

---

[28] Black, *supra* note 1, at 297.

[29] The Wassenaar member countries are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States. *Participating States*, WASSENAAR ARRANGEMENT, http://www.wassenaar.org/participants/index.html (last visited Mar. 29, 2013).

[30] Corr, *supra* note 27, at 455 (quoting Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Guidelines & Procedures, including the Initial Elements (Dec. 2011), *available at* http://www.wassenaar.org/guidelines/docs/5%20-%20Initial%20Elements.pdf) (internal quotation marks omitted).

[31] *Cf.* Bert-Jaap Koops, *Crypto Law Survey*, CRYPTO LAW SURVEY, http://www.cryptolaw.org/cls2.htm#ab (last updated Feb. 2013).

[32] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies , Dual-Use List – Category 5 – Part 2 – "Information Security", at 87 (Dec. 2012), *available at* http://www.wassenaar.org/controllists/2012/WA-LIST%20%2812%29%201/08%20-%20WA-LIST%20%2812%29%201%20-%20Cat%205P2.doc

[33] *Id*. at 85.

[34] *See id*.

[35] *See* Corr, *supra* note 27, at 455.

[36] Black, *supra* note 1, at 298. Although the U.S. has never placed restrictions on domestic

restriction on the importation of cryptography systems.[37] The exportation of encryption products, however, has historically been heavily restricted, and although the restrictions have been eased in recent years in many respects, the regulations still present obstacles and risks to U.S. businesses operating overseas.[38]

1. Regulations on Use

¶17 The U.S. does not restrict the domestic use of cryptography. Furthermore, a federal district court has held that there is no obligation to reveal one's encryption key or password in the context of a criminal investigation.[39] However, a recent case has held that, while a defendant cannot be compelled to provide his or her decryption key or password, he or she can be compelled to provide unencrypted copies of the files or documents in question under certain circumstances. [40] In *United States v. Fricosu*, law enforcement agents recovered a laptop with a hard disk that was password-protected and encrypted.[41] The government sought a warrant to allow it to search the laptop, and also sought a writ pursuant to the All Writs Act, 28 U.S.C. § 1651, that would require the defendant to produce the unencrypted contents of the computer.[42] The defendant declined, asserting her privilege against self-incrimination under the Fifth Amendment.[43] The Court found that the laptop in question belonged to the defendant, or, in the alternative, that she was its sole or primary user, and was able to access the encrypted contents.[44] Reasoning that "there [was] little question . . . but that the government [knew] of the existence and location of the computer's files," the court held that there was no incriminating testimonial evidence that would be revealed by compelling the defendant to produce the unencrypted documents.[45]

2. Regulations on Export

¶18 The export of encryption products from the United States is regulated by a variety of governmental agencies. The primary regulator of encryption exports is the Commerce

---

cryptography use, during the 1990s the Clinton Administration pursued several initiatives that sought to subject cryptography to more control, particularly for law-enforcement purposes. The most infamous of these initiatives was the Clipper Chip program, which sought to create a standard for voice encryption that would have allowed government agents to decrypt encrypted voice communications. However, after lobbying by both the IT industry and privacy advocates the program was essentially abandoned, and the U.S. government endorsed the free and unrestricted domestic use of cryptography. *See* Vandana Pednekar-Magal & Peter Shields, *The State and Telecom Surveillance Policy: The Clipper Chip Initiative*, 8 COMM. L. & POL'Y 429, 430 (2003).

[37] Koops, *supra* note 31.

[38] *See* section IV.A, *infra*.

[39] In *In re Grand Jury Subpoena to Boucher*, the Federal District Court of Vermont "held that the act of being compelled to turn over an encryption password has testimonial aspects [and therefore a] defendant [is] allowed to refuse to surrender his password under protection of the Fifth Amendment right to refrain from testimonial self-incrimination." Brendan M. Palfreyman, Note, *Lessons from the British and American Approaches to Compelled Decryption*, 75 BROOK. L. REV. 345, 353 (2009) (footnotes omitted).

[40] United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012).

[41] *Id.* at 1234.

[42] *Id.* at 1235, 1237.

[43] *Id.* at 1235.

[44] *Id.* at 1235–36.

[45] *Id.* at 1237.

Department's Bureau of Industry and Security (BIS), which administers the Export Administration Regulations (EAR). [46] The EAR govern the export of any dual-use commodities, including encryption systems.[47]

¶19 Encryption products are regulated under Category 5, Part 2 of the EAR.[48] Generally, if an item to be exported uses or contains cryptography, is not designed for medical end use, and does not limit the use of cryptography to intellectual property or copyright protection functions (as with a DVD), then the item is regulated under Category 5, Part 2.[49] The regulations governing cryptography export have been relaxed in recent years,[50] but still require exporters to determine for themselves the licenses and other documentation required for their software exports, taking into account the software to be exported, the person or entity to whom the software is being sold, and additional factors.[51]

¶20 The first factor exporters must consider is the attributes of the software to be exported. One primary consideration is key length: Category 5, Part 2 specifies that encryption systems with key lengths of 56 bits or less for symmetric systems, or 512 bits of less for asymmetric systems, can be exported without restriction;[52] however, those key lengths represent weak encryption, and strong encryption systems, which must use longer keys, face export restrictions.[53] Furthermore, there is an exemption for so-called "mass market" encryption products; if an encryption product is generally available to the public, for home or personal use, without continuing support by the supplier (e.g., a personal

---

[46] *See* John F. McKenzie, *U.S. Export Controls on Internet Software Transactions*, 44 INT'L LAW. 857, 858 (2010).

[47] *Id.*

[48] Bureau of Industry and Security, Export Administration Regulations, Commerce Control List, Category 5—Telecommunications and "Information Security" (Dec. 7, 2012), *available at* http://www.bis.doc.gov/policiesandregulations/ear/ccl5_pt2.pdf.

[49] *Id.* There are other, more specialized exemptions to Category 5, Part 2 control. For example, Note 4 exempts from regulation items that meet all of the following conditions:

> a. The primary function or set of functions is not any of the following:
> 1. 'Information security';
> 2. A computer, including operating systems, parts, and components therefor;
> 3. Sending, receiving or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records management); or
> 4. Networking (including operation, administration, management and provisioning);
> b. The cryptographic functionality is limited to supporting their primary function or set of functions; *and*
> c. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs a. and b. above.

Id. at 1–2. However, the uses of cryptography central to this article—securing data and communications for business and personal purposes—do not fall into this exemption, and hence Note 4 will not be considered in detail here.

[50] *See, e.g.*, Department of Commerce, Bureau of Export Administration, Revisions to Encryption Items (Jan. 10, 2000), *available at* http://epic.org/crypto/export_controls/finalregs.pdf.

[51] *See* McKenzie, *supra* note 46, at 858-59.

[52] Bureau of Industry and Security, *supra* note 48, at 4.

[53] For this reason, until recently it was common to find encryption software available in two versions: one version with "weak cryptography" (56 or 512 bits) that was available for general export, and another version with "strong cryptography" with limited exportability. However, as export restrictions have generally been relaxed, it is now less common to find such dual versions of cryptography software.

email security program), then its export is not restricted by this section.[54] A final important exemption is for products "*when accompanying their user for the user's personal use or as tools of the trade . . .*";[55] this allows users to, for example, travel with laptops and mobile phones that contain encryption capabilities (as essentially all do).

¶21 A second important factor for exporters to consider, and that is much more difficult for exporters to control, is to whom the software is being sold. This includes the specific attributes of the customer and the customer's location. The Office of Foreign Assets Control (OFAC), an agency within the U.S. Treasury Department, administers sanctions programs against specific countries, restricting the export of sensitive products and materials—including cryptography software—to those locations.[56] In addition, OFAC administers restrictions against exports to specially designated individuals and entities, known as "Specially Designated Nationals" ("SDNs"); exports to those individuals and entities are generally prohibited.[57]

¶22 These requirements have become even more onerous with the advent of electronic software delivery. Whereas it used to be common for software to be physically delivered to the customer (e.g., on a CD-ROM), it is now more common for software products to be made available for download via the Internet. Generally, U.S. export regulators do not distinguish between physical shipment and electronic delivery when determining whether a firm has made an illegal export.[58] Firms that sell encryption software over the Internet, therefore, must take steps to screen their customers to assure that they are neither located in an embargoed country nor are SDNs. Unfortunately, it is as yet unclear what kinds of steps such firms can, or should, take to ensure compliance.[59] Although restrictions on export of cryptography have been relaxed, the regulatory environment has, if anything,

---

[54] This is specified in Note 3:

[The cryptography software regulations] do not control items that meet all of the following:
a. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
1. Over-the-counter transactions;
2. Mail order transactions;
3. Electronic transactions; or
4. Telephone call transactions;
b. The cryptographic functionality cannot be easily changed by the user;
c. Designed for installation by the user without further substantial support by the supplier; and
d. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs (a) through (c) of this note.

Bureau of Industry and Security, *supra* note 48, at 1.

[55] *Id.*

[56] *See* Corr, *supra* note 27, at 461. Currently, OFAC administers comprehensive sanctions against Burma (Myanmar), Cuba, Iran, Sudan, and Syria. Additionally, OFAC administers non-comprehensive sanctions programs against the Western Balkans, Belarus, Cote d'Ivoire, the Democratic Republic of the Congo, Iraq, Liberia, Libya, North Korea, Somalia, and Zimbabwe. *Frequently Asked Questions and Answers*, U.S. DEPARTMENT OF THE TREASURY, http://www.treasury.gov/resource-center/faqs/Sanctions/Pages/answer.aspx (last updated July 25, 2013).

[57] *Frequently Asked Questions and Answers*, *supra* note 56.

[58] *See* McKenzie, *supra* note 46, at 860.

[59] *Id.* at 859.

become more challenging; recent years have seen a "shifting of export control responsibilities from the government to the private sector."[60] As one commentator noted:

> Today's private entities have much greater responsibility for ensuring compliance with any applicable regulations. The penalties for non-compliance are severe, and lesser involvement by the agencies on the regulatory side has made government resources available on the enforcement side. Therefore, more than ever before, private entities must make sure they have internal compliance or export management systems in place to avoid or minimize export control violations.[61]

¶23 U.S. firms selling or operating abroad must take steps to ensure that they do not violate U.S. export regulations whenever their operations involve the use of encryption—and, increasingly, this applies to every major firm.

C. Cryptography Regulation in the European Union

¶24 Cryptography in the European Union (EU), like in the U.S., is free to use domestically, but faces restriction on its export. Export of dual-use goods—which includes cryptography—is regulated by Council Regulation (EC) No. 1334-2000. These regulations follow the Wassenaar Arrangement. Export within the European Union is fully liberalized. Exports to a select group of non-EU countries are lightly regulated, and exports to remaining countries are more heavily regulated.[62]

¶25 The European Union has been a long-time advocate of free domestic use of strong cryptography. In the 1990s, the Clinton Administration pursued several international initiatives aimed at encouraging—or even mandating—key escrow.[63] The EU, through the European Commission, took a stance against those proposals.[64] The Commission "stresse[d] the economic and societal importance of cryptography," and noted that "[k]ey escrow or key recovery raise a number of practical and complex questions that policy makers would need to solve, in particular issues of privacy, vulnerability, effectiveness and costs."[65] Hence, European support for the free use of encryption and opposition to mandatory key escrow proved critical to the continued development of strong cryptography.

---

[60] Corr, *supra* note 27, at 491–92.

[61] *Id*.

[62] *Dual Use Controls*, EUROPEAN COMMISSION, http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/index_en.htm (last updated July 8, 2013). The countries for which the lighter regulations apply are the United States, Canada, Japan, New Zealand, Switzerland, and Norway. *Id*.

[63] Mandatory key escrow would have required that copies of all encryption keys be kept on file with a trusted third party. This way, if the government wanted access to an individual's or entity's communications (e.g., for law enforcement purposes), they could obtain a court order for the trusted third party to reveal the keys.

[64] Black, *supra* note 1, at 302.

[65] Koops, *supra* note 31 (internal quotation mark omitted).

D. Cryptography Regulation in China

¶26 China is one of the most challenging environments for cryptography use and regulation. Importation and exportation of cryptography products are both highly regulated. Import and export of encryption products require a license from the State Encryption Management Commission.[66] Encryption is regulated primarily by the National Commission on Encryption Code Regulations (NCECR). Encryption products cannot be sold or imported in China without prior approval by NCECR.[67] Furthermore, individuals and firms in China can only use cryptography products approved by the NCECR.[68] This also applies to foreign individuals and firms operating in China, who must report details of their encryption systems to, and receive approval to use those products from, the NCECR.[69] One scholar has reported that, "[a]ccording to a 'clarification letter' sent to US businesses in China in early March 2000," the restrictions on import and use of cryptography involve:

> only hardware and software for which encryption and decoding operations are core functions. As a result, products in which cryptography is only built-in (such as mobile phones and browser software) are exempted. . . . However, the clarification letter only seems to apply to pre-2000 products. All products since 2000 seem to require a license.[70]

¶27 However, according to the international law firm Baker & McKenzie, the clarification letter has been disavowed by Chinese authorities, and, for practical purposes, all encryption products, regardless of key strength or other factors, are fully regulated.[71]

¶28 In addition to restricting the import and use of encryption technologies to those firms that have received governmental approval, the Chinese government has in many instances pursued a policy of favoring the development of domestic cryptography systems. An important example of this involved systems for secure wireless local area network (LAN) connectivity. The international standard for wireless connectivity, used almost everywhere worldwide, is the 802.11 standard promulgated by the Institute of Electrical and Electronics Engineers (IEEE).[72] However, in 2003, the Chinese government announced the creation of a new Chinese standard for wireless LAN security—the WLAN Authentication and Privacy Infrastructure (WAPI)—and stated that wireless LAN (or Wi-Fi) systems sold in China would have to conform to the WAPI, not

---

[66] Shangyong Mima Guanli Tiaoli (商用密码管理条例) [Regulation of Commercial Encryption Codes] (promulgated by the State Council, Directive No. 273, Oct. 7, 1999, effective Oct. 7, 1999) (China), *available at* http://newmedia.cityu.edu.hk/cyberlaw/gp3/pdf/law_encryption.pdf.

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] Koops, *supra* note 31.

[71] Baker & McKenzie, *New Chinese Tariff Classifications for Encryption Products*, CHINA LEGAL DEV. BULL., April-June 2009, at 11, 12, *available at* http://www.amchamchina.org/download?path=/cmsfile/2009/06/24/551b9aab50bbd64c3f33a7913ea3d9ce.pdf.

[72] Yang, *supra* note 26, at 908.

the 802.11, standard.[73] Furthermore, foreign companies that wished to sell Wi-Fi devices in China would have to co-produce their products with designated Chinese firms.[74]

¶29 The WAPI standard was heavily opposed by international IT firms, largely because they saw it as a protectionist tool used by the Chinese government to favor their own domestic technology producers.[75] Another reason for opposing WAPI, however, was the fear that the domestic cryptography standard would create a functional key escrow system that would allow the Chinese government easier access to encrypted communications. The WAPI episode indicates that the Chinese government will continue to be heavily involved in the market for, and in the use of, cryptography technologies in China.

IV. IMPACTS OF CRYPTOGRAPHY REGULATIONS

¶30 Restrictions on cryptography have deleterious effects on at least three groups: (1) information technology and security companies wishing to compete in international markets; (2) firms operating abroad that desire to use cryptography to protect their data and communications; and (3) individuals and groups in countries with restrictions on use of cryptography who would like to protect their data from corporate or government interference.

A. Effects on IT Industry

¶31 Varying cryptography regulations worldwide place substantial burdens on information technology and security firms looking to expand into new markets. Many analysts believe that U.S. export controls have placed American IT firms at a competitive disadvantage vis-à-vis foreign competitors.[76] Furthermore, all IT and security firms—not just those based in the U.S.—face increased costs due to compliance with foreign import requirements. Finally, to the extent that encryption regulations in major markets (e.g. China) constrain demand for cryptography services in those countries, security firms are disadvantaged.

¶32 The effects of cryptography regulations on IT firms extend beyond the market for cryptography software, however. Many information technology products, services, and businesses depend upon strong cryptography. For example, e-commerce (exemplified by Amazon.com in the U.S.) would not have flourished had customers feared that every time they made a purchase online, they were placing their credit card information at risk of compromise; yet this fear would be justified in the absence of strong cryptography to protect the information in transit. By limiting the use of cryptography, countries hinder the development of their IT and e-commerce markets in general.

---

[73] Yang, *supra* note 26, at 908, 912–15.

[74] *Id.* at 914.

[75] *Id.* at 909, 916. The administration of President George W. Bush agreed, and it successfully lobbied China to delay indefinitely the introduction of WAPI as a mandatory standard. *Id.* at 915–17.

[76] *See, e.g.*, Black, *supra* note 1, at 297.

B. Effects on Overseas Business Activities

¶33 Restrictions on importation and use of cryptography have substantial effects on the operations of multinational firms. Network managers for firms in the West tend to design encryption technologies into their voice and data networks to protect the contents of their telephone calls, emails, documents, and databases; however, when they wish to use these same technologies abroad, they must tailor their systems to the restrictions of each country in which they operate, or they may violate local laws and regulations.[77] These difficulties are amplified where laws are unclear or inconsistently enforced, a situation common in many developing countries. As Bruce Schneier, a noted encryption expert, observed, "Rules are often hard to find and hard to follow [because] governments want people not to do anything."[78]

¶34 China presents a particularly difficult case. As discussed above, Chinese encryption regulations have often been volatile and vague. While Chinese restrictions on cryptography facially apply to foreign firms doing business in China, "[a]ccording to attorneys familiar with the matter, Chinese officials say the encryption restrictions are aimed at Chinese citizens, not foreign corporations."[79] Nevertheless, "companies can expect the Chinese government to ask for details about the encryption they're using—in addition to requiring them to appoint an 'encryption contact' who will give the government the encryption keys when asked."[80] The Vice President for Security Services at one multinational firm noted, "We have part of our business in Beijing. . . . If you encrypt data in China, you have to provide the Chinese government the ability to access the keys. By this regulation, the Chinese should be able to get access to [Secure Sockets Layer]-encrypted traffic, too."[81] Because of these restrictions, he noted that many businesses do not use encryption in China, even if cryptography is a standard component of their IT infrastructure elsewhere.[82] China is far from alone in having opaque and inconsistent encryption regulations; in Russia, where the Federal Agency of Governmental Communications and Information has issued regulations requiring government approval to use encryption, "the interpretation of the rules seem to vary according to which government official you contact . . . ."[83]

¶35 Restrictions on the import and use of cryptography affect businesses in several important ways. If firms cannot use encryption devices to secure their data and communications in a given country, then their intellectual property in that country is put at substantial risk. The situation is perhaps even worse where regulations are unclear and inconsistently applied, as is the case in China, Russia, and elsewhere; in such situations, a firm must decide between avoiding cryptography but exposing its data to compromise, and using cryptography but exposing itself to sanctions. Such regulatory uncertainty will tend to favor well-connected firms at the expense of market newcomers, undermining the competitiveness of the market and discouraging new entrants.

---

[77] Ellen Messmer, *Encryption Restrictions*, NETWORK WORLD (Mar. 14, 2004, 10:05 PM), http://www.networkworld.com/careers/2004/0315man.html.

[78] *Id.* (internal quotation marks omitted).

[79] *Id.*

[80] *Id.*

[81] *Id.* (alteration in original).

[82] *Id.*

[83] *Id.*

C. Effects on Organizations and Individuals in Highly-Regulated Countries

¶36 Finally, it should not be forgotten that limitations on the use of cryptography by individuals and organizations remove a potent tool to preserve privacy and communicate in the face of governmental opposition. Encryption makes it far easier for human rights advocates, dissent movements, and the like to communicate and organize.[84] Where encryption software is unavailable or illegal, these movements will find it much harder to organize, and this can have deleterious effects on the promotion of socially valuable change.

V. RECOMMENDATIONS AND BEST PRACTICES

¶37 Best practices for American firms operating abroad encompass two aspects: (1) compliance with U.S. export regulations, and (2) compliance with foreign import and use regulations.

A. Compliance with U.S. Export Regulations

¶38 Because of the complex nature of U.S. export regulations, and the harsh penalties for violating those regulations, any major American company operating abroad that either sells products that include cryptography, or utilizes cryptography in its lines of business, should institute internal compliance programs. The U.S. Commerce Department's Bureau of Industry and Security encourages internal compliance programs to incorporate particular components, including: (1) "a written corporate policy statement discussing the importance of compliance with all export control laws and regulations"; (2) internal procedures for correctly classifying all products according to their applicable regulatory classifications, and for ensuring that these classifications are communicated to salespeople; (3) procedures for screening customers against both the lists of prohibited/restricted countries, and the lists of prohibited individuals and entities (Specially Designated Nationals); (4) programs for monitoring the activity of the firm's U.S. persons and subsidiaries abroad, and also the activities of the firm's foreign affiliates;[85] (5) step-by-step clearance procedures that must be undertaken before delivery of a product, and keeping record of those procedural steps for each delivery; (6) training and auditing for relevant personnel; (7) due diligence in corporate transactions, including foreign mergers and acquisitions;[86] and (8) procedures for notification and enforcement in

---

[84] *See* ALEX COMNIOS, ASS'N FOR PROGRESSIVE COMMC'NS, *TWITTER REVOLUTIONS AND CYBER CRACKDOWNS: USER-GENERATED CONTENT AND SOCIAL NETWORKING IN THE ARAB SPRING AND BEYOND* 15, 17 (2011), *available at* http://www.apc.org/en/system/files/AlexComninos_MobileInternet.pdf.

[85] Corr, *supra* note 27, at 516-18.

> Under OFAC regulations, U.S. companies and U.S. persons in those companies may risk liability if their overseas affiliates engage in transactions with embargoed countries and OFAC decides the U.S. companies or persons participated. Likewise, . . . BIS could arguably impute liability to U.S. companies or persons if an overseas affiliate ships to a prohibited end-use or end-user, and BIS decides the U.S. persons should have known."

Id. at 518.

[86] *Id.* at 518–20.

> BIS announced in late 2002 that 'corporations will be held accountable for violations of U.S. export control laws committed by companies that they acquire.' This warning makes clear

case of any violations or suspected violations.[87] None of the components are simple to implement, but they are all necessary in light of the substantial penalties that can result from even inadvertent illegal export.

¶39 In addition to ensuring that the firm's customer-facing practices are in compliance with U.S. export regulations, a firm must also take steps to prevent internal systems—particularly IT systems—from allowing for inadvertent violations of export law. For purposes of U.S. regulations, the term "export" includes: "(1) transmission of data and software by email or otherwise over a computer network to foreign access points; (2) posting or storing information on a computer network such as a company intranet site or a shared library, folder, or database, if persons outside the United States have access; and (3) access of foreign nationals both abroad, and on-site in the United States, to network data and software."[88] Therefore, simply making software available from a central server for installation on networked PCs—a standard configuration for company networks—could place the firm in violation of export regulations if that software contains strong cryptography and the firm networks are accessible from foreign locations. Corr recommends a four-part compliance program for managing such systems: (1) identify all data and software on the network that could be subject to export controls; (2) segregate the data and software that are subject to control (for example, by placing them on a separate network drive); (3) restrict non-U.S. persons and entities from access to those segregated areas; and (4) "[d]irect [r]equests for [a]ccess to [c]ontrolled [t]echnologies to [d]esignated [i]n-[h]ouse [c]ompliance [m]anagers."[89]

B. Compliance with Foreign Encryption Regulations

¶40 While compliance with U.S. export regulations is complicated enough, compliance with foreign encryption regulations presents a great deal more difficulty. Many countries do not have clear regulations or guidelines for importation, exportation, and use of encryption, and even those countries that have clear guidelines often suffer from inconsistent enforcement. It is therefore extraordinarily important to develop country-specific policies that address the particular regulatory environment in each country, the firm's particular needs in that country, and the risks associated with eschewing cryptography in that jurisdiction.

¶41 Where a firm decides not to use cryptography in a given country, it must take additional steps to protect its data and intellectual property from compromise. One of the most important considerations is the selection of networking connectivity provider. Where a firm or individual can utilize strong cryptography to protect communications over the network, the trustworthiness and reliability of the network provider are less

---

> that, although the focus of export compliance programs is on day-to-day-operations, the breadth and scope of U.S. export controls also may reach larger, higher-level corporate transactions. Multinational corporations, as well as financial companies such as commercial and investment banks, are well-advised to implement due diligence compliance measures in connection with mergers, acquisitions, and joint ventures, as well as distribution, licensing, and sales agreements.

Id. at 520 (footnote omitted).

[87] *Id.* at 520.

[88] *Id.* at 522.

[89] *Id.* at 522–25.

relevant. However, where data—including email and voice communications—must be sent unencrypted over the network, choosing a network provider that is both trustworthy, and has strong security systems and procedures of its own in place, is of paramount importance.

¶42 Additionally, where a firm chooses not to use encryption, it should act to minimize the amount and sensitivity of the data accessible from within the country. The first part of such a program should be determining what data do and do not need to be accessible to in-country staff; data that do not need to be available in-country should be moved to secure locations (e.g. to a data center in the firm's home country) and made inaccessible to in-country employees (so that data do not travel over unsecured network links). Data that need to be accessible to in-country employees should be divided between data that are *only* needed by in-country employees or data that are needed enterprise-wide. The former should be stored locally, on-premise, at the in-country business entity, so that the data are not disseminated over insecure communications links. Where the firm has multiple in-country locations, at least some data would likely need to be shared among offices, but as much data as possible should be stored off-network.

¶43 Where a firm in a country with restrictions on cryptography and implied governmental rights to decryption keys (like China) chooses to use encryption, it should nevertheless take measures that it would not take in the U.S., Europe, or other locations. Because the government in such countries can demand access to decryption keys, those keys should never be used to protect, or to grant access to, sensitive enterprise information. Furthermore, encryption keys for in-country users should be changed regularly, and old keys should be expired at a faster rate so that the compromise of a given key provides access to less data.

VI. CONCLUSION

¶44 Cryptography is essential for the secure operation of nearly all organizations, and is key to protecting the privacy of individuals worldwide. Despite its importance, however, and despite the fact that many countries place strong restrictions on the use of cryptography, too many organizations neglect to consider the regulatory implications of cryptography use in their international organizations. All internationally active firms must take steps to ensure that they are in compliance with encryption regulations in all countries where they do business, and at the same time must adopt best practices to maximize their information security in spite of restrictions on cryptography use.