The legality of online Privacy-Enhancing Technologies

Éloïse Gratton[*]

[*] Attorney at the Mendelsohn Rosentzveig Shacter Law Firm. Email : egratton@mrslaw.com

TABLE OF CONTENTS

INTRODUCTION

1. The use of the Internet will spread widely in coming years and commerce on the World Wide Web will boom.[1] We expect to be able to buy products easily from home over the Internet and have access to all kinds of information sources. The well-known concern is that browsing the Internet will create detailed databases describing each user's browsing patterns and that third parties will then be able to assemble comprehensive profiles about online users. The information about the user is gathered through the collection of transactional data, Internet tracking, and tracking IP addresses.[2] Companies and third parties collect a variety of personal information including name, email, address, telephone number, credit card number, Social Security number, age or date of birth, gender, education, occupation, income, hobbies, interests, and the type of hardware or software used by the online consumer.[3] The information is then stored in customer lists, databases for marketing programs, cookies, bugs, etc., therefore breaching the privacy of the online users.

2. Privacy has been defined as the "The right to be left alone"[4] and interpreted by the German Court in 1983 as "Information self-determination."[5] In a more modern society, privacy is more likely to be defined as "Personally Identifiable Information" (PII) which is information that can be linked to a specific individual like a name, an address, data elements such as date of birth and zip code, or a transactional history and that can narrow the focus down to a small group of defined people. Privacy is about user control over their personal information, over collection and use of personal data, about disclosure of information to third parties and about the possibility of having a proper recourse in the case of breaches.

3. Privacy on the Internet has arisen as one of the leading consumer concerns. In given studies, it appeared that 85% of online users regard the privacy of information transmitted online as the most important issue on the Internet[6] and 87% of Internet users are concerned with threats to their individual privacy while online.[7]

4. These Internet users are not wrong in their concerns if we consider recent privacy abuses. *Toys R Us* used a third party web log analysis service without disclosing this fact and was served with a class action suit for breaching its privacy policy.[8] *Toysmart*, who had initially promised not to sell data to third parties, decided to sell data anyhow as it went bankrupt, so the *Federal Trade Commission* had to intervene and stop the transaction.[9] Finally, the Double Click scandal occurred when it was revealed that after the online company's database was merged with the *Abacus Direct* database marketer, the company intended to sell the 100,000 online user profiles it had compiled without the users' knowledge.[10]

5. In order to solve privacy problems and make sure companies are obligated to comply with privacy laws or more specifically with the standards established by the European Commission, many companies similar to *Zero-knowledge Systems Inc.*[11] and *Anonymizer.com*[12] are or have been marketing privacy-enhancing technologies in order to protect and assure the privacy of the individual in the digital world.

6. The Freedom software version 2.0[13] created by *Zero-knowledge* and the *Anonymizer*[14] software created by *Anonymizer.com*, like most of these online privacy-enhanced technologies, use a method called encryption, which scrambles the data, making it illegible to everyone except the intended recipient. The goal has been to create mathematically rigorous systems that will prevent even the most determined attackers from discovering the user's identity, therefore significantly reducing the risk of data theft or accidental leaks of sensitive information from the Internet user's computer.[15]

7. While these privacy tools do help to protect the privacy of the Internet users in making sure that data collectors comply with the European Privacy Directives,[16] a further analysis may determine that these software programs are illegal according to Canadian, American or French encryption control laws and regulations.

1. Privacy-Enhancing Technologies (PETs)

8. In order to minimize the collection of Internet users' personal data and help solve the problem of

online privacy, companies like *Zero-knowledge* and *Anonymizer.com* have developed the following online privacy tools:

1.1 Zero-knowledge Freedom 2.0 software

9. *Zero-knowledge*, with offices both in Montreal and San Jose, California has emerged as one of the market leaders in privacy-enhancing technology. *Zero-knowledge* was founded in 1997 by Hammie, Austin, and Hamnett Hill in Montreal, Quebec. Their mission has been to develop and market technologies that will protect the privacy of the individual in the digital world.

10. They launched their consumer product "Freedom" in December 1999 and declared that it was the only comprehensive consumer privacy product to protect individuals on the Internet. Freedom 2.0 was eventually released and was offering, until recently, the additional option to add enhanced premium services, such as untraceable encrypted e-mail, anonymous Web browsing and anonymous chat.

11. While Zero-knowledge has stopped providing anonymous Web browsing and encrypted pseudonym e-mail services since October 2001.[17] its then-available version 2.0 of the Freedom software was providing a complete security tool for Internet users that had features and technical descriptions that may be similar to other Internet privacy-enhancing technologies, including *Anonymizer*[18] (that will be further analyzed in this paper), net *HUSH*,[19] *Idzap*,[20] *Ponoi*,[21] *PrivacyX*,[22] *Private Idaho*,[23] *Rewebber*,[24] and *Siege Surfer*.[25]

1.1.1 Features of the Freedom 2.0 software

12. The **Personal Firewall** function protected the user's computer against malicious intruders. A firewall is a combination of hardware and/or software that separates a Local Area Network, which is a computer network limited to the immediate area, into two or more parts for security purposes.

13. The **Form Filler** function speeded up and secured online registrations and transactions. It automatically filled out forms, making online registrations and purchases quick. It also remembered login passwords to save the user time.

14. Every browser[26] is assigned an ID number. That ID number is held in a file called a cookie. That number is not attached to a name, just a number. Thousands of sites use cookies to enhance the user's Web viewing experience. Cookies cannot damage user files, nor can they read information from a user's hard drive. Cookies allow sites and advertisers to "remember" users across pages of a site and across multiple visits to a site. This feature facilitates e-commerce and Internet advertising in numerous ways, including: allowing personalization features such as stock portfolio tracking and targeted news stories, allowing shopping cart capabilities and quick navigation across multiple zones of e-commerce sites, remembering user names and passwords for future visits, and delivering advertisements targeted to a user's interests.[27]

15. The **Cookie Manager** function prevented web sites from tracking the user's activities and enabled the users to control the cookies they receive. It automatically erased the user's tracks by deleting cookies third parties could employ to assemble comprehensive dossiers of their customer profiles and spending patterns.

16. The **Ad Manager** function controlled ads and speeded up browsing, eliminated distractions and prevented activity-tracking cookies and "Web bugs" from being dropped onto the user's computer. This could be used to control ad frequency or the number of times a user sees a given ad (spam[28] control).

17. The **Keyword Alert** prevented personal information from leaving the user's computer. It instantly scanned all outgoing communications for sensitive information and warned the user before sending anything that contains it. For example, the user could program Freedom to scan for his real name or telephone number and Freedom would alert the user before releasing it.

18. For users demanding the highest level of online security and privacy protection, Freedom offered additional premium services to ensure the most secure and private Internet experience available.

19. The **Untraceable Encrypted E-mail** function secured and privatized the user's e-mail, an essential feature for those needing to send important and sensitive information with absolute security. Freedom's "military-grade" encrypted e-mail system worked with the user's existing e-mail account to ensure that no one, including the user's ISP, could intercept and read the user's messages. Freedom also blocked unsolicited bulk e-mail (spam) from reaching the user's inbox.

20. Finally, the **Anonymous Browsing and Chat** function provided the user with a tool to go online undetected. This function erased the tracks the user leaves when he browses the Web and posts to newsgroups or chat rooms.

1.1.2 Description of the Freedom 2.0 software

21. The Freedom 2.0 Internet Privacy Suite was made up of the following three components: Network + Nym + Strong Encryption = Internet Privacy.[29]

22. The Freedom **Network** created private routes between the user's computer and the destination computer. Freedom was automatically re-routing data through a series of globally distributed servers known as the Freedom Network. This private network was acting as a cloak to provide the Internet user with anonymous connections to the Internet. Freedom servers had no way of matching the original source with the ultimate destination of the user's mail or Web connections. Freedom worked transparently alongside the user's existing browser and did not require the user to change ISPs.

23. Pseudonymisation is the process of changing personal data by using an attribution algorithm in such a way that it is impossible to link individual details of a personal or commercial nature to an individual without knowing or being able to use that algorithm.[30] Freedom 2.0 was letting the online user create multiple online identities by means of pseudonymous nicknames called **nyms**. The user could employ nyms to interact on the Internet but the nyms could never be traced back to the user.

24. Switching from one nym to another was quick and easy and allowed the user to separate private interests from its true identity. When using Freedom's premium services, all mail and Web communications were encrypted and sent through the Freedom Network. No one, including the user's ISP, could associate the user's nyms with the user's true identity.

25. According to Zero-knowledge, marketing companies were unable to compile an accurate profile of the user's online browsing habits. Also, malicious hackers were unable to intercept, read and link the user's e-mail messages to his true identity and no one was able to monitor the user's sensitive personal information.

26. Finally, Freedom 2.0 used "**Strong encryption**" of 128-bits on all incoming and outgoing Internet traffic.[31]

1.2 *Anonymizer.com* software

27. *Anonymizer.com* is a San Diego-based company founded in 1996 and is a pioneer of Internet privacy technologies. It is one of the most popular and trusted names in online privacy services. Its mission is to ensure that going online does not compromise an individual's right to privacy.

28. *Anonymizer* acts as a shield between the Internet user and all of the most prevalent online privacy and security threats.

1.2.1 Features of the Anonymizer software

29. The **Anonymous Web Surfing** service rewrites the web pages the Internet user wants to view on his protected servers and removes privacy and security threats from web pages before serving them to the user. It also hides the Internet user's unique IP address from web sites and other outside parties, preventing them from seeing the user's browsing.

30. The service **blocks cookies** and prevents outside parties from putting malicious files or code on the user's hard drive.

31. The **Safe Cookies** function makes it safe to accept cookies from sites that require them, for example for shopping, sign-ups, personalized content, etc., without worrying about long-term tracking. *Anonymizer* converts long-term cookies sent to the Internet user by Web sites into session-only, automatically expiring cookies. These cookies are encrypted by the *Anonymizer* to ensure intermediaries cannot read them and are rewritten so as to be session-only, so that they are not stored permanently on the Internet user's computer.

32. The **URL Encryption** function scrambles the Internet user's Web page requests so that third parties (including the user's boss, ISP or co-workers with access to the user's Internet connection) are not able to log them.

33. The **Ad Filtering** function removes standard-size banner ads from the user's page views for faster and more secure surfing.

34. The Anonymizer Secure Tunneling Service, on top of the above-mentioned features, provides Anonymous Newsgroup access and the **Anonymous Email** function to enable online users to send anonymous e-mails.

35. It is interesting to note that Freedom 2.0 provided similar features to *Anonymizer*, and a comparative analysis of these software is available on *Anonymizer.com*'s website.[32]

1.2.2 Description of the Anonymizer software

36. The **Anonymizer surfing** provides a secure encrypted connection to the Anonymizer's servers and enables the Internet user to surf anonymously with the Cookie Encryption feature (that lets the Internet user safely access and use Web sites that require cookies) and the URL Encryption feature (that encrypts the Internet user's page requests so that their ISP are not able to log them). The service also blocks cookies, Java, JavaScript, and other tracking methods and provides Anonymous Instant Messaging and Anonymous Newsgroups. URL encryption is achieved through the use of 128-bits encryption.[33]

37. When a user connects normally to the Internet, his transactions are relayed through several servers before reaching their final destination. These servers have the ability to collect information as the user's requests are routed through them.[34] Since the user's requests are not encrypted, any server between the user and his final destination could see what the user is doing. The **Secure Tunneling** service--that can be used independently of, or transparently in conjunction with Anonymizer Surfing--creates a virtually impregnable tunnel from the online user's computer to Anonymizer's servers, and encrypts the Internet activity between the Internet user's computer and the Anonymizer's servers. This prevents any servers between the user and Anonymizer, such as the user's ISP, from monitoring the user's activities.

38. Anonymizer Secure Tunneling account function allows the user to encrypt his incoming and outgoing e-mail, surf and news posts through a method known as "port forwarding". Secure Shell ("SSH") is a program that encrypts everything about the message and sends it to the Anonymizer servers. Since SSH does port forwarding, a third party monitoring the Internet user's connection will not be able to tell that what the user has sent was mail. When the message is received by the Anonymizer's servers, the message is decrypted and sent "as normal" to the recipient. Anonymizer uses the most

popular encryption algorithms of 128-bits to provide Internet users with this function.[35]

39. Finally, the **Anonymizer Dialup Access** service provides the features of Anonymous Web Surfing and Anonymizer Secure Tunneling but also lets Anonymizer become the Internet user's ISP connection.

1.3 Encryption

40. Traditionally, cryptography was almost exclusively reserved for the domain of governments. Cryptography protected military or diplomatic secrets and was predominantly embedded in hardware.

41. As previously mentioned, Freedom 2.0 used "Strong encryption" of 128-bits on all incoming and outgoing Internet traffic[36] and Anonymizer uses the exact same strength of encryption to provide Internet users with the URL encryption feature[37] and to encrypt Internet traffic.[38]

42. Encryption scrambles the user's data, making it illegible to everyone except the user's intended recipient. Cryptographic methods provide encryption, decryption, and digital signatures. Encryption provides for confidentiality: keeping information protected from unauthorized disclosure or viewing by mathematically scrambling the original text. Digital signatures, which are analogous to written signatures in that they are an electronic identifier created by a computer and attached to an electronic document, provide other functions like authentication (proof that users are who they claim to be), non-repudiation (proof that a transaction occurred or that a message was sent or received), and integrity (so that data cannot be modified without detection).

43. There are two major cryptographic methods. In Secret Key cryptography, the same key is used to encrypt and decrypt the data. This type of cryptography requires both parties to pre-arrange the sharing of the single key that is used for both encryption and decryption.

44. In Public Key cryptography, there are two different but related keys and what is encrypted with one can only be decrypted by the other. Each user has a private key and a public key. The private key is kept secure, known only to the user, the other key can be made public and either sent over the network to each correspondent or placed in a secure public directory. To use this kind of system, the sender would encrypt a message with the recipient's public key, and only the recipient's private key could decrypt the message. Public key cryptography thus permits the secure transmission of data across open networks such as the Internet without the necessity of previously exchanging a secret key. This allows parties who do not know each other to exchange and authenticate information and conduct business in a secure manner and this represents the method used by Freedom 2.0[39] and Anonymizer.[40]

45. Without access to the correct key, data encrypted to ensure confidentiality can only be decrypted into understandable data by trying all possible variations of the key and checking to see if the result is meaningful. All other things being equal, cryptographic strength is defined by the length of the cryptographic key (or bit-length) and determines the number of possible permutations. With each bit added to the length of the key, the strength is doubled. It is estimated that it would take well over 13 billion times the age of the universe to crack a 128-bit key like the one used by Zero-knowledge or Anonymizer.com in their software.[41]

2. Privacy

46. Internet Service Providers and managers of Local Area Networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally systematically "log" in a file the date, time, duration and IP address given to the Internet user. The same can be said about the Internet Service Providers that keep a logbook on the http server. In these cases there is no doubt about the fact that one can talk about "personal data" in the sense of article 2 a) of the Directive 95/46/EC.[42] In other cases, a third party can get to know the IP address of a user but not be able to link it to the other data concerning this person that would make their identification possible.

47. The likelihood exists in many cases, however, of linking the user's IP address to other personal

data, whether such data is publicly available or not, that will identify the user, especially if use is made of invisible processing means to collect additional data on the user. For instance, the data collector could be using cookies containing a unique identifier or a modern data mining system linked to large databases containing personally identifiable data on Internet users.

48. Therefore, even if it may not be possible to identify a user in all cases and by all Internet actors from the data processed on the Internet, the possibility of identifying large masses of personal data of the Internet user exists in many cases .

2.1 European Directives

49. The general data protection Directive 95/46/EC applies to any processing of personal data[43] falling within its scope, irrespective of the technical means used. Personal data processing on the Internet, therefore, has to be considered in light of this Directive.[44]

50. The specific Directive 97/66/EC on the protection of privacy and personal data in the telecommunications sector particularizes and complements the general Directive 95/46/EC by establishing specific technical and legal provisions. Directive 97/66/EC applies to the processing of personal data in connection with the provision of publicly available telecommunications services. The Internet thus forms part of the public telecommunications sector.[45] Directive 95/46/EC applies to all matters that are not specifically covered by Directive 97/66/EC.[46]

2.1.1 Data Quality

51. The EC data protection Directive 95/46/EC contains two principles which have direct consequences for the design and use of new technologies: its “finality” or “purpose” principle requires that personal data only be used where necessary for a specific legitimate purpose.[47]

52. The Directive states that personal data must be processed fairly and lawfully,[48] collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.[49] The data must be adequate, relevant, not excessive in relation to the purposes for which they are collected and/or further processed,[50] accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete (keeping in mind the purposes for which they were collected or for which they are further processed) are erased or rectified.[51]

53. A user shall be entitled, fee of charge, to be omitted from a printed or electronic directory at the user’s request and to indicate that the user’s personal data may not be used for the purpose of direct marketing.[52]

54. The “finality” or “purpose” principle mentioned above is the underlying motive for the concept of Privacy-Enhancing Technologies.[53] This concept refers to a variety of technologies, like the Freedom or the Anonymizer software, that safeguard personal privacy, notably by minimizing or eliminating the collection or further processing of identifiable data.[54]

55. As a matter of fact, each of Freedom 2.0 and Anonymizer aims to hinder any unlawful forms of processing by, for instance, making it technically impossible for unauthorized persons to access personal data, so as to prevent the possible destruction, alteration or disclosure of these data.

56. Freedom 2.0 is based on the use of a so-called identity protector that may be regarded as an element of the system that controls the release of an individual’s true identity to various processes within the information system. Its effect is to cordon off certain areas of the system that do not require access to true identity. Several other techniques are used by the software to introduce an identity protector into an information system including, among others, encryption techniques involving digital signatures. Anonymizer hides the Internet user’s unique IP address from web sites and other outside parties, preventing them from seeing the user and preventing outside parties from putting malicious files

or code on the user's hard drive.

2.1.2 Consent and Data Access

57. According to the European Directives, personal data may be processed only if the data subject has unambiguously given his/her consent.[55] Also, the data collector must provide a data subject from whom data relating to himself are collected with the purpose of the intended processing[56] (except where the subject already has it) and any further information, such as the existence of the right of access and the right to rectify data concerning the subject.[57]

58. Also, the data subject has to have the right to object, on request and free of charge, to the processing of personal data relating to him/her which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on his/her behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.[58]

59. Each of Freedom 2.0 and Anonymizer safeguards personal privacy, notably by minimizing or eliminating the collection or further processing of identifiable data[59] therefore making these concepts irrelevant since no personal data will be collected at any time (at least no relevant data that could be useful to a third party like a marketing company).

2.1.3 Data Security and Confidentiality

60. When it comes to the issues of confidentiality and security, data controllers must take appropriate measures to protect the information supplied by their customers against unauthorized access or disclosure, in particular when the process involves the transmission of data on a network, as is the case with electronic transactions on the Internet. These measures must take into account the risks to security and confidentiality, the nature of the data, and state-of-the-art technology.[60]

61. Everyone has the right to send mail to others without that mail being read by a third party. Article 5 of Directive 97/66/EC lays down obligations as to the confidentiality of communications. In addition to these obligations, Article 4 of the same Directive obliges the providers of telecommunications services to take appropriate technical and organizational measures to safeguard the security of their services and to inform users about a particular risk of a breach of security and any possible remedies, including the costs involved.

62. In the off-line world, everyone has the ability to send a letter anonymously or under a pseudonym. In order to be able to send anonymous e-mail, the user could obtain an anonymous e-mail address from several providers of such a service. Freedom lets the online user create multiple online identities using pseudonymous nicknames called nyms so that the user may use nyms to interact on the Internet but the nyms can never be traced back to the user. Anonymizer hides the Internet user's unique IP address from web sites and other outside parties, preventing them from knowing the user's identity and also enables the users to surf anonymously, send anonymous e-mails and have anonymous Newsgroups access. It also provides the Cookie Encryption feature that lets the Internet user safely access and use Web sites that require cookies.

63. From the user's point of view, a number of issues are relevant depending on the type of e-mail: confidentiality, integrity and authentication. Confidentiality is the protection of the transmitted data to prevent eavesdropping and one possible way to guarantee confidentiality is encryption of the message to be sent. Integrity, which is a guarantee that information is not altered accidentally or on purpose, can be obtained by calculating a special code on the basis of the text and transmitting this special code which is then encrypted along with the text itself. Authentication, which guarantees that a user is who he/she claims to be, can be verified by exchanging digital signatures based on digital certificates. These certificates do not need to mention the real name of the user and instead can mention pseudonyms, as stipulated in Article 8 of the Electronic Signature Directive.[61]

64. For security and confidentiality purposes, each of the Freedom 2.0 and the Anonymizer software uses full-strength encryption on Internet traffic[62] or on the connection to the Anonymizer's servers to enable the Internet user to surf anonymously[63] while offering a feature that blocks unwanted cookies. This significantly reduces the risk of data theft or accidental leaks of sensitive information from the user's computer and in some cases provides proof that users are who they claim to be, as well as non-repudiation (proof that a transaction occurred or that a message was sent or received), and integrity, so that data cannot be modified without detection.

2.2 Privacy-Enhancing Technology Companies

65. It may be obvious that Privacy-Enhancing Technologies developed by companies like Zero-knowledge or Anonymizer.com are useful in the protection of the privacy of online users. At the same time it is still to be determined if these companies are promoting privacy through their business model, when they have or may have access to personal information related to their customers.

2.2.1 *Zero-knowledge*

66. Zero-knowledge's vision on privacy is the following:

> "*Everyone has the right to control their personal information. Only you should have the right to decide what people know about you. Freedom gives you total control over your private and sensitive information on the Internet, allowing you to decide who gets to know what about you.*"[64]

67. According to *Zero-knowledge*, two different parties have audited Freedom in order to make sure that *Zero-knowledge* is not gathering data about their users. It has also released its entire source code to the Freedom client base and has begun to release the source code to the Freedom Network. Its system is designed so that no one, including *Zero-knowledge*, knows the true identity behind a Freedom user's online pseudonymous identity (nym). This is made possible by its activation code purchasing system, which separates personally identifying information from nyms, making any sort of association between the two impossible. The only information that can apparently be recovered by *Zero-knowledge* is the information related to when the nym was created or renewed, the number of messages sent by the nym, the e-mail address, and date of sent messages.

2.2.2 *Anonymizer.com*

68. Anonymizer.com's vision of privacy is based on Article 19 of this fifty-year-old document that the Internet has made more applicable than ever:

> "*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*"[65]

69. On its website, more specifically under the section entitled "Account Policies", *Anonymizer.com* states that it considers the Internet user's e-mail address to be confidential information and that it will never rent, sell or otherwise reveal it to others without the user's prior consent.[66] It further mentions that, while it does hold the necessary billing information on certain users (those, for example, who pay by credit card), this information could in no way be correlated with the user's Internet activities, since its billing system and the *Anonymizer.com* services run totally independently of each other. It also advertises that anonymous cash payment is available to purchase its services and products.[67]

70. *Anonymizer.com* further states that it maintains no information that would identify which user had sent a given message or visited a given site and that it does not store phone numbers, addresses or other information that would help identify users.[68]

3. Encryption

71. Cryptography is the transformation of data by a mathematical formula called a key, rendering data unintelligible for anyone without the right key. Cryptographic technologies provide a foundation for establishing trust in electronic commerce or web browsing because they safeguard information, protect communications, and authenticate parties to transactions.

72. Encryption has implications both for electronic methods of doing business, public safety, and national security and it can protect sensitive or personal information, support electronic commerce, prevent theft of sensitive data, and protect intellectual property.

73. But the very elements that make cryptography attractive for reasons of privacy, competition, human rights, and business security can also conceal activities which pose a threat to public safety since it is equally true that cryptographic technologies could be used to hide criminal activity and to threaten national security. Criminals and terrorists could use cryptography to thwart the legally-mandated information-gathering abilities of law enforcement and security agencies. The inability to access or to decrypt information could well have a significant impact on the prevention, detection, investigation and prosecution of crime.

74. For this reason each country has laws and regulations related to cryptographic products, whether it is according to its import or export control regulations, or according to the regulations regarding the domestic use of such products.

75. Privacy-Enhancing Technologies like Freedom 2.0 or Anonymizer are available through *Zero-knowledge*'s Canadian and *Anonymizer.com*'s United States web sites for downloads and purchases by anyone having access to the Internet. A European customer looking to purchase such privacy tools from North American web sites may be found in breach of the French laws, given that France may have more restrictive encryption control policies. For this reason, it may be interesting to compare Canadian standards with the American or the European standards regarding encryption control.

3.1 Canada

76. Until recently, customized encryption software or hardware products with a key length of 40 bits or less were exportable even if banking and financial institutions were permitted to export 56-bit DES[69] products. On December 24, 1996, Canada modified its policy for a twelve-month trial period to allow export of 56-bit customized encryption software or hardware with embedded encryption to most countries. This was then extended for another six months[70] until the new Canadian policy was put in force in order to respond to the changes in the global supply of, and demand for, cryptography products.

77. Canada was previously a member of the *Coordinating Committee for Multilateral Export Controls*[71] (COCOM), an international organization for the mutual control of the export of strategic products and technical data from country members[72] to proscribed destinations. It maintained, among others, the International Industrial List and the International Munitions List. In 1991, COCOM decided to allow export of mass-market cryptographic software, including public domain software.

78. The main goal of the COCOM regulations was to prevent cryptography from being exported to countries considered "dangerous", usually the countries thought to maintain friendly ties with terrorist organizations, such as Libya, Iraq, Iran, and North Korea. Exporting to other countries was usually allowed, although states often required a license to be granted.

79. COCOM was dissolved in March 1994. Pending the signing of a new treaty,[73] most members of COCOM agreed in principle to maintain the status quo and cryptography remained on export control lists.

3.1.1 Export/ import controls

80. Canada does not currently restrict or control the import, production or use of any strength of cryptographic products within Canada.

81. Canada, previously a member of COCOM, now has export commitments pursuant to the *Wassenaar Arrangement*[74] *on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*. The Wassenaar Arrangement is a thirty-three-nation[75] international protocol established in 1996 which restricts the export of hardware, some software cryptography products, and products that use cryptography. It was created on the basis of the Initial Elements 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, thus preventing destabilizing accumulations. Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals and are not diverted to support such capabilities.

82. Consequently, in February 1998, a discussion *White Paper by the Task Force on Electronic Commerce*[76] entitled "A Cryptography Policy Framework for Electronic Commerce"[77] was released for discussion. The White Paper stressed the importance of accessible cryptography as a building block for electronic commerce.[78] Immediately following this publication, the government announced a new cryptography policy on October 1, 1998, and Industry Minister John Manley affirmed the government's commitment to the Wassenaar Arrangement by announcing the elements of Canada's Cryptography Policy.[79] The Policy is a component of the *Canadian Electronic Commerce Strategy* and it permits Canadians to develop, import and use whatever cryptography products they wish and does not impose mandatory key recovery requirements or a licensing regime. The policy encourages the growth of electronic commerce, allows Canadian producers to export their products globally within the framework of international arrangements, and contains measures to maintain the capability of law enforcement agencies to ensure public safety.

83. The official federal policy on cryptography[80] announced in October of 1998[81] outlined the six following elements:[82]

84. Canadians should be free to develop, import and use whatever cryptography products they wish;

85. The government will not impose mandatory key recovery requirements or licensing regimes for certification authorities or trustees;

86. The government will encourage industry-based use and modeling of responsible cryptography practices and will act as model user, through its current public key infrastructure (PKI) initiative;[83]

87. Export controls will comply with the Wassenaar Arrangement, the goal being to maintain a level playing field for Canadian cryptography manufacturers against those of other countries;

88. The government intends to streamline the export permit process and make it more transparent; and

89. Legislative amendments will be introduced to protect consumer privacy while providing a legal framework for law enforcement and national security agencies. More specifically, the government proposes amendments to the Criminal Code and other statutes as necessary to criminalize the wrongful disclosure of keys, deter the use of encryption in the commission of a crime, deter the use of cryptography to conceal evidence and apply existing interception, search and seizure and assistance procedures to cryptographic situations and circumstances.

90. Moreover, warrants and assistance orders also apply to situations where encryption is encountered to obtain the decrypted material or decryption keys.[84]

91. These guidelines for the export of information and security-related equipment and technologies that

are reflected in hardware and software dual-use lists are found in the *Export Control List*[85] and, more specifically, in Group 1 of the Control List. These export controls are authorized by the *Export and Import Permits Act*. According to the Commerce/NSA report, the *Export and Import Permits Act*[86] (EIPA), the *Export Control List*[87] (ECL) and the *Area Control List* (ACL) are the mechanisms by which Canada controls exports. The EIPA authorizes the government to exercise export controls to ensure that military or strategic goods are not exported to destinations representing a strategic threat to Canada. The Ministry of External Affairs is responsible for the implementation of the Act.

92. The Minister of Foreign Affairs,[88] pursuant to subsection 7 (1.1) of *the Export and Import Permits Act*, has issued the annexed General Export Permit No. 39 that covers the "Mass market cryptographic software" on June 1, 1999. This Permit defines the term "Mass market cryptographic software" as:

> "*Mass market cryptographic software means the goods referred to in Group 1 of the schedule to the Export Control List that are described in item 1154*[89] *of the Guide and that meet all of the following conditions:*
>
> - *generally available to the public by being sold, without restriction, from*
> - *stock at retail selling points by any of the following means: (i) over-the-counter transactions, (ii) mail order transactions, (iii) electronic transactions, or (iv) telephone transactions;*
> - *the cryptographic functionality cannot easily be changed by the user;*
> - *designed for installation by the user without further substantial support by the supplier; and*
> - *does not contain a symmetric algorithm employing a key length exceeding 128 bits*."

93. Any resident of Canada may, under the authority of and in accordance with this Permit, export mass market cryptographic software from Canada[90] even though the Permit does not authorize the exportation of mass market cryptographic software to any country listed in the Area Control List or any of the following countries:[91] North Korea, Iran and Iraq.[92] Additionally, the countries of Angola, the Federal Republic of Yugoslavia, and Myanmar have been included on the Canadian Area Control List since 1999.[93] For this reason it is presently illegal to download cryptographic software from one or all of these countries or redistribute cryptographic software to these countries.

3.1.2 Domestic laws and regulations

94. There are no domestic regulations on cryptography so Canadian individuals and firms are free to use and trade any strength of encryption throughout Canada.[94]

3.2 United States of America

95. The United States government has long been the leader in limiting the development and dissemination of encryption. For the past twenty years, this country has attempted to suppress development of encryption through manipulating standards, recommending legislation, and imposing export controls. In the past several years, as electronic commerce has become an important aspect of the American economy, the U.S. government has begun backing away from these efforts, which have not been successful and had generated considerable controversy and opposition. Finally, in January 2000, the Administration announced a new export policy that relaxed many controls.

3.2.1 Export/ import controls

96. There are no import restrictions on cryptography in the United States. On the exporting side, the U.S. has signed the Wassenaar Arrangement but has not implemented the pre-December 1998 General Software Note and generally maintains stricter controls.

97. Export controls on commercial encryption products are administered by the *Bureau of Export Administration* (BXA) in the U.S. Department of Commerce. Rules governing exports of encryption are found in the Export Administration Regulations.[95]

98. Cryptography export used to be controlled by the *International Traffic in Arms Regulation* (ITAR).[96] At the end of 1996, cryptography export was transferred to the Export Administration Regulations of the Department of Commerce where the export policy was relaxed to favor export of data-recovery cryptography[97] and encryption rules are now published by BXA since that transfer.[98] The Department of Justice is now included in crypto export decisions.[99] Making cryptography available on the Internet is considered export, unless appropriate measures are taken to prevent foreigners from accessing the cryptography.

99. As previously mentioned, the U.S. government, after many years of delay, has begun to relax export controls of encryption products. In January 2000 the government announced changes to the Export Administration Regulations concerning the export of cryptographic products[100] after evaluating many different requirements for cryptographic exports.[101] The earlier announcement permitted cryptographic exports to certain business sectors in certain countries and eliminated the requirement for key recovery mechanisms to be included in exports.

100. The new regulations were published on January 12, 2000,[102] but on October 19, 2000, the *Bureau of Export Administration* (BXA) published a rule implementing the Administration's announcement on July 17, 2000,[103] therefore amending the January 2000 regulations.

101. The new regulations of January 2000 and October 2000 largely eliminated the sector and country limitations and also brought some changes to the prior regulations. Now any encryption commodity or software, including components, of any key length can be exported under a license exception after a technical review by the BXA to any non-government end-user in any country except for the seven state supporters of terrorism.[104] Exports previously allowed only for a company's internal use can now be used for any activity, including communication with other firms, supply chains and customers. Previous liberalizations for banks, financial institutions and other approved sectors are continued and subsumed under the license exception.[105]

102. Any encryption item, including commodities, software and technology, of any key length may be exported to foreign subsidiaries of U.S**.** firms without a technical review.[106] All items produced with encryption commodities, software, and technology authorized under this license exception will require a technical review only for items to be re-exported, resold or transferred.[107]

103. Exports to government end-users may be approved under a license unless the destination is a foreign government member of the European Union or one of eight selected countries.[108] This last license exception was included during the first policy update in 2000, since the Administration was committed to ensure that U.S. exporters would not be disadvantaged by steps taken by the European Union (EU) in the creation of a "free-trade zone". As a matter of fact, the October rule's major change tracks with the recent regulations adopted by the EU by permitting most encryption products to be exported to the fifteen EU member states and eight additional trading partners under a license exception.[109]

104. Also, the October rule allows the release of consumer products incorporating short-range technologies, streamlines reporting requirements, liberalizes the export of commercial source code, clarifies the treatment of object code compiled from source code considered publicly available, and allows procedures for the release of certain products from U.S. Content Requirements. U.S. exporters can ship products immediately after filing a commodity classification request without waiting for the technical-review results or the previously used thirty-day delay period.[110]

105. The policy[111] was adopted in response to the changing global market, advances in technology and the need to give the U.S. industry better access to these markets, while continuing to provide essential protections for national security.

3.2.2 Domestic laws and regulations

106. There are no domestic use controls on cryptography in the United States so American individuals and firms are free to use and trade any strength of encryption throughout the United States.

3.3 France

107. France has a long history of regulating the use of cryptography. Prior to 1990, France considered cryptographic products "war materials" and generally prohibited their use with some exception. Before 1996, delivery, importation, exportation, and use of cryptography were subjected to (a) prior declaration, if the cryptography could have no other objective than authenticating communications or assuring the integrity of transmitted messages and (b) prior authorization by the Prime Minister in all other cases.

108. Simplified procedures existed for certain cryptography products or services or certain user categories. For authorization, a file containing technical details and administrative data had to be submitted and such authorization could be subjected to certain conditions in order to reserve the use of certain types of cryptography to defined user or application categories.

109. On June 18, 1996, the French legislature passed a new law on cryptography, "Loi de réglementation des télécommunications"[112] which amended the 1990 law.[113] Decrees on the application of the law were published on February 25, 1998,[114] and several more decrees were also published on March 13 and 23, 1998.[115] The law slightly liberalized the use of authentication-only encryption but also introduced the requirement for *Trusted Third Party* (TTP) systems. A TTP is an independent third party who is trusted by both the user and the service provider, similar to a digital attorney.[116] This party can be trusted with keeping such things as the master key linking digital pseudonyms with the true identities of their users. The trusted party knows that the relationship between a user's true identity and his pseudo-identity must be kept completely secret. However, if certain conditions require it, the trusted party will be permitted to reveal the user's identities to a service provider or to law enforcement authorities. The only authorized *Trusted Third Party* or *Key Escrow Agency* (KEA) was SCSSI,[117] according to a decree on March 13, 1998.[118]

110. In that decree it was proposed that cryptography that did not provide confidentiality could be used without restriction, so the prior requirement of declaration would be cancelled while the supply of authentication-only cryptography still had to be declared. However, both use and supply of confidentiality cryptography still required authorization. Decree 98-206[119] specified categories of cryptography, which did not require a declaration or an authorization.[120] A supplier would be exempted from the formalities for use exclusively for developing, validating, or demonstrating cryptography if he informed SCSSI at least two weeks in advance. A supply authorization for collective use exempted users from acquiring use authorization. The use of cryptography with key lengths limited to 40 bits would be exempted from declaration according to decree 98-207.[121]

111. However, the law was never enacted and the new Socialist government of Prime Minister Lionel Jospin seemed to change course on France's strict policies on cryptography usage.

3.3.1 Export/ import controls

112. France signed the Wassenaar Arrangement for export controls in December of 1998, with the exception of the pre-December 1998 General Software Note, so it controls the export as well as the import and use of encryption products. French encryption controls are administered by the *Service Central de la Sécurité des Systèmes d'Information* (SCSSI), an office reporting to the Prime Minister through the *Secrétariat Général à la Défense Nationale* (SGDN). This reflects a general French view that technology and industrial policy are critical elements of national defense.[122]

113. At a press conference on January 19, 1999, Prime Minister Jospin announced the liberalization of the domestic crypto legislation.[123] In March 1999 the French government released the relevant decrees

to implement relax controls on encryption. The decrees allow for the use of encryption up to 128 bits, raised from 40 bits, as well as relax requirements that keys be placed with "Trusted Third Parties". These changes were implemented in Decrees 99-200[124] and 99-199,[125] pending the implementation of the law which is to offer full liberalization of crypto use.

114. The import from countries outside the EU and the EEA (*European Economic Area*) and export of cryptography is regulated according to the law of 26 July 1996[126] and the decrees implementing it of 24 February 1998,[127] and of 17 March 1999.[128]

115. Decree 99-200 of March 17, 1999, that replaced the decrees 98-206 and 98-207 of March 23, 1998, specifies categories of cryptography that do not require any prior formality. Decree 99-199 of March 17, 1999 specifies categories of cryptography for which prior declaration is required, instead of prior authorization.

116. For cryptographic products with key length up to 40 bits, there is no formality for importation.[129] For products between 40 to 128 bits, there is no formality for importation except in the event that such importation is for a physical person who will use the product for confidentiality purposes.[130] In the event that it is not the case, a declaration will be required by the user wishing to import the said product.[131]

117. Also, for cryptographic products with key length up to 128 bits, the user needs an authorization prior to exporting the said product.[132]

118. Export of dual-use goods, including cryptography, is regulated by the *Council Regulation* (EC) No 1334/2000[133] setting up a community regime for the control of exports of dual-use items and technology and replacing the earlier 1994 Council Regulation.[134]

119. Export to other EU countries and within the EU is entirely liberalized, with the exception of some highly specialized products, such as cryptanalysis items. For these items, member states can issue General Intra-Community Licenses valid for export to one or more determined EU countries provided basic requirements are met, such as a statement of the end use of exported items. For re-exports after intra-EU export, an information-exchange mechanism is established.

120. For export to Australia, Canada, the Czech Republic, Hungary, Japan, New Zealand, Norway, Poland, Switzerland and the United States, a *Community General Export Authorization* (CGEA) can be applied for, which is valid for export from all EU countries.

3.3.2 Domestic laws and regulations

121. France has restricted the domestic use and supply of cryptography for a long time. Restrictive legislation where authorization and declaration were required for almost all cryptography was slightly liberalized in 1996 and the domestic use of cryptography was further liberalized in January 1999. As a matter of fact, there is no formality to personally use a cryptographic product that is between 40 to 128 bits in France, except if the end user is a physical person who will personally use the product.[135] If this is not the case and the product will be used simply for confidentiality purposes, a declaration is required.[136]

122. The *Association des Utilisateurs d'UNIX et de Systèmes Ouverts*[137] surveyed over 200 French companies and released a white paper in January 2000.[138] A majority of the companies felt that they were still placed at a competitive disadvantage because of the French law. Only five percent of the respondents provided their keys to a "Trusted Third Party." The groups called for the full relaxation of controls on encryption and the development of encryption standards to facilitate electronic commerce. For this reason, a law on "Information Society" is currently being drafted that would fully relax encryption controls which is expected to be approved this year.

4. The legality of online Privacy-Enhancing Technologies

123. The "finality" or "purpose" principle established by the European Directives[139] is the underlying

motive for the concept of Privacy-Enhancing Technologies[140] like the Freedom and the Anonymizer software, that safeguard personal privacy, notably by minimizing or eliminating the collection or further processing of identifiable data.[141] These privacy tools aim to hinder any unlawful forms of processing by making it technically impossible for unauthorized persons to access personal data, so as to prevent the possible destruction, alteration or disclosure of these data.

124. This makes most of the principles and standards established by the European Directives irrelevant since no personal data will be collected at any time, at least no relevant data that could be useful to a third party.

125. Freedom 2.0 lets the online user create multiple online identities using pseudonymous nicknames called nyms. The user can then use nyms to interact on the Internet without the nyms being traced back to the user, taking into account the principles of confidentiality of communications established by the Directives.[142] Anonymizer also protects the confidentiality of its customers by scrambling the Internet user's Web page requests so that no third parties with access to the user's Internet connection are able to log them. It further promotes confidentiality with its Anonymous Email and Anonymous Newsgroup access features.

126. Finally, each of Freedom 2.0 and Anonymizer uses full-strength encryption on Internet traffic[143] and/or on the Internet user's connection to the Anonymizer's servers[144] and provides a feature that blocks unwanted cookies therefore significantly reducing the risk of data theft or accidental leaks of sensitive information from the user's computer, which is in line with the principle of data security established by the European Directive.[145]

127. While each of the Freedom and the Anonymizer software can be quite useful to protect the privacy of the Internet users, anonymity on the Internet can be viewed as threatening. In a recent *Study on Legal Aspects of Computer-Related Crime in the Information Society*,[146] it was outlined that technical solutions and measures against the abuse of anonymity on the Internet should be taken. Another perceived threat can be seen where non-repudiation services based on certified pseudonyms and the certification authority is able and obliged to furnish the name and address of the holder of the pseudonym under clearly defined circumstances.

128. For this reason, *Zero-knowledge* requires that the use of the Freedom software comply with all applicable laws and regulations, including all applicable local, provincial, state, national, and international laws and regulations and including all laws relating to copyright, trademark, obscenity, defamation, the right of privacy, false advertising, threats of violence and incitation of hate and fraud.[147] *Anonymizer.com* requires that its software shall not be used for sending commercial e-mail solicitation, harm computer systems, threaten someone, send mass e-mailings, obtain unauthorized access to any computer system, furtherance of criminal activity and other illegal activities.[148]

129. In a general way, the Freedom 2.0 and the Anonymizer software are legal if the user or customer is careful to obey the intellectual property and export rules, as well as any local rules that may apply in the nation they are in. A legal disclaimer on the Freedom website states the following:

> "*Zero-knowledge Systems makes no representation that materials on the Freedom Site are appropriate or available for use in other locations, and accessing them from locations where their contents are illegal is prohibited. Those who choose to access the Freedom Site from other locations (than Canada) do so on their own initiative and are responsible for compliance with local laws*."[149]

130. As for Anonymizer, although the site does specify under the user agreement section that the customer certifies that they are not under-age,[150] they do not specify that those who choose to access their site or purchase their products and services, from other locations than the United States, do so on their own initiative and are responsible for compliance with local laws. It is interesting to note that after contacting the Anonymizer website IRC chat support services to determine if their products were legal in

foreign countries,[151] the author did not receive a clear answer and was referred to the www.fsecure.com.[152]

131. While Freedom and Anonymizer do help in protecting the privacy of Internet users, it is to be determined if these privacy tools are legal according to laws regulating cryptographic products in Canada, in the United States and in France.

4.1 Canada

132. Canada does not currently restrict or control the import, production or use of any strength of cryptographic products within Canada so for this reason it is generally legal to import the Anonymizer software.

133. It is also legal to export the Freedom software from Canada, without a license, to non-government end-users. However, there are restrictions with regards to Angola, the Federal Republic of Yugoslavia and Myanmar that are listed in the Area Control List as well as North Korea, Iran and Iraq.[153]

134. To that effect, the Freedom software website states the following:

> "*Legal contract:*
> *Canadian law prohibits us from allowing the download of* ***cryptographic software*** *from countries on Canada's Area Control List. I am not downloading this software from a country on Canada's Area Control List. I will not redistribute this software to a country on the Area Control List. I understand that downloading or distributing this software to a country on the Area Control List is a violation of Canadian law."*[154]

135. For this reason, it is presently illegal to download Freedom 2.0 from one or all of these countries or redistribute the software to these countries.

136. There are no domestic regulations on cryptography. Also, there are no laws restricting the private use of cryptography so Canadian individuals and firms are free to use and trade the Freedom or the Anonymizer software throughout Canada.

4.2 United States of America

137. There are no import restrictions on cryptography in the United States so it is legal to import the Freedom software to the United States from any country or to purchase the Anonymizer software from such country.

138. Since the new regulations of 2000, a Privacy-Enhancing Technology such as the Anonymizer software can now be exported from the United States under a license exception after a technical review by the BXA to any non-government end-user in any country except for the seven state supporters of terrorism.[155] Exports of the Anonymizer software from the United States to government end-users may be approved under a license unless the destination is a foreign government member of the European Union or one of the eight selected countries.[156]

139. On this issue, while *Anonymizer.com* mentions in the user agreement found on its website that such agreement is governed by and will be construed in accordance with the laws of the State of California, United States of America,[157] it does not specify, as previously mentioned, that the United States prohibits certain countries from downloading the software and that those who choose to access the Anonymizer.com site from other locations than the United States do so on their own initiative.

140. Anonymizer can be exported or re-exported to foreign subsidiaries of U.S. firms without a technical review.[158] Finally, there are no domestic use controls on cryptography in the United States so anyone is free to use Freedom or Anonymizer within the country.

4.3 France

141. France used to be quite restrictive, but now the nation allows its citizens to use strong cryptography, recognizing its value in preventing some crimes and strengthening electronic commerce.

142. There is no formality to import the Freedom or the Anonymizer software in France only in the event that such importation is for a physical person that will use the product for confidentiality purposes.[159] In the event that it is not the case, a declaration will be required by the user wishing to import the said software.[160]

143. As for exporting from France software that would have a similar technical description to the Freedom or Anonymizer software, the user will need an authorization prior to exporting such software.[161] Exporting software similar to Freedom 2.0 or Anonymizer within the EU is liberalized[162] and for export to Australia, Canada, the Czech Republic, Hungary, Japan, New Zealand, Norway, Poland, Switzerland and the United States, a *Community General Export Authorization* (CGEA) can be requested, which is valid for export from all EU countries.

144. The domestic use of cryptography was recently liberalized and there is no formality to personally use the Freedom or Anonimyzer software, only if the end user is a physical person who will have a personal use of the product.[163] If this is not the case and the Freedom or the Anonymizer software will be simply used for confidentiality purposes, a declaration is required.[164]

CONCLUSION

145. An analysis of the export and import controls in Canada, in the United States and in France as well as an analysis of the regulations regarding the domestic use of cryptographic products in these countries established that--in a general way and only recently--Freedom 2.0 and Anonymizer are legal except in limited cases. Even if we consider that the strength of encryption used in these tools would make them legal in a country like Canada, the actual "use" of the software could be illegal. As a matter of fact, the software could be used to infringe copyright and trademark laws, to promote obscenity and defamation, to abuse the right of a third party's privacy, to promote false advertising or hate and fraud, therefore making the use of the software illegal.

146. Zero-knowledge was promoting the fact that its Freedom 2.0 software would give the online users total control over the disclosure of their private and sensitive information since it would let the users manage their privacy and choose whether they wish to reveal their identity or remain private, depending on the situation. It also invoked the fact that the users could, while using its software, express themselves online and visit their favorite web sites without worrying about who was tracking or profiling their online activities and they could also block malicious hackers from accessing their computer system and decide who could send them e-mail, virtually eliminating abuse and online spam.

147. Online Privacy-Enhancing Technologies suggest that cryptography should be deployed widely to assure security in the transmission of data in order, for example, to prevent a malicious party from obtaining credit card numbers or any other personal information online.

148. Cryptography is important to the growth of electronic commerce because it allows users to authenticate and safeguard sensitive data such as credit card numbers, electronically signed documents, personal e-mail and other information stored in computers or transmitted over closed or public networks such as the Internet. Cryptography can also be used in a wide range of applications, from the government communicating securely with citizens to the ensured confidentiality of medical records in hospital databases.

149. On the one hand, encryption is crucial for information security and for protecting privacy, but on the other hand, full anonymity may be undesirable in particular circumstances, such as those associated with criminal activity where legitimate reasons exist to identify the individual. Governments are trying

hard to address these conflicts of interest, but up to now their proposals for regulation have been controversial. The policy debate is polarized, with privacy activists and law-enforcement agencies fiercely opposing each other's point of view.

150. Ian Goldberg, Chief Scientist at Zero-knowledge, suggests that instead of putting their faith in privacy laws, online users should use privacy-enhancing technologies in order to protect their privacy online. He recently stated: "The law of the land can be changed by the next administration. The laws of mathematics are more rigid."

[1] Federal Trade Commission, “Self-Regulation and Privacy Online: A report to Congress”, July 1999, p. 1.

[2] An IP address is an address that relates to a computer or device on a TCP/IP network like the Internet. Data is routed through the Internet based on the destination IP address.

[3] Federal Trade Commission, “Privacy Online: A Report to Congress”, June 1998, p. 24.

[4] Warren and Brandeis, The Right to Privacy, 1890 Harvard Law Review.

[5] German Court 1983, Concept of confines (Prof. Umberto Eco).

[6] @Plan/Yahoo! Internet Poll, March 6, 2000.

[7] Beyond Concern: Understanding Net Users’ Attitudes About Online Privacy, AT&T, April 14, 1999.

[8] Olsen, Stefanie, Staff Writer, CNET News.com: “Toysrus.com drops tracking service amid pressure”, August 14, 2000. http://news.cnet.com/news/0-1007-200-2520471.html.

[9] Federal Trade Commission, “FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website visitors”, July 10, 2000. http://www.ftc.gov/opa/2000/07/toysmart.htm.

[10] Privacy Foundation, “Workplace Surveillance is the Top Privacy Story of 2000”, DoubleClick Unplugged. http://www.privacyfoundation.org/release/top10.html.

[11] http://www.zeroknowledge.com.

[12] http://www.anonymizer.com.

[13] http://www.freedom.net.

[14] http://www.anonymizer.com.

[15] Industry Canada, Stratégie canadienne, Groupe de travail sur le commerce électronique: “Le commerce électronique au Canada, Vie privée: Protection des renseignements personnels”, 10 décembre 2000. http://e-com.ic.gc.ca/francais/privee/632d21.html.

[16] More specifically Directive 95/46/EC and Directive 97/66/EC.

[17] Featherly, Kevin, “Web Anonymity Service Dumped By Zeroknowledge”, Newsbytes, October 4, 2001. http://www.newsbytes.com/news/01/170843.html.

[18] The service allows the Internet user to browse the Internet using an intermediary to prevent unauthorized parties from gathering his personal information. http://www.anonymizer.com/.

[19] The software enables anonymous browsing and the protection of the Internet user’s identity. http://nethush.com/.

[20] It provides free anonymous surfing and other services available for subscription. http://www.idzap.com/.

[21] It provides a personal, portable privacy platform. Consumers access Ponoi through a web browser on any networked computer and can surf the Web, use their passwords and store files without compromising their privacy to ISPs, employers, Web sites. http://www.ponoi.com/.

[22] It allows Internet users to send and receive e-mail with anonymity, privacy and security.

https://www.privacyx.com/www/.

[23] The Internet privacy utility for Windows simplifies using e-mail with PGP, anonymous re-mailers, and nym servers, providing the Internet user with more electronic privacy.
http://www.eskimo.com/~joelm/pi.html.

[24] It provides different services to protect the Internet user's privacy while browsing the Web. http://www.rewebber.de/.

[25] The creator of a line of privacy and security enhancing software, Siege Soft, allows the Internet user to access the Internet anonymously with its Siege Surfer.
http://www.siegesoft.com/_html/home.asp?jsEnabled=true.

[26] The browser being the vehicle by which a computer accesses the Internet.

[27] Netscape, "Cookies: what they are and how they work", February 26, 1997.
http://help.netscape.com/kb/consumer/19970226-2.html.

[28] For more information regarding online spam, see : Gauthronet, Serge and Drouard, Étienne, Commission of the European Communities, "Unsolicited Commercial Communications and Data Protection" – Summary of Study Findings, Internal Market DG – Contract no ETD/99/B5-3000/E/96, January 2001.

[29] http://www.freedom.net.

[30] Schulz, Gabriel, "Privacy-enhancing technologies", Working Document by the Working Group on "privacy enhancing technologies" of the Committee on "Technical and organizational aspects of data protection" of the German Federal and State Data Protection Commissioners, October 1997, p. 5.

[31] Freedom system 2.0 Architecture, December 18, 2000.

[32] http://www.anonymizer.com

[33] http://www.anonymizer.com, URL Encryption FAQ.

[34] The most common example of a server that can collect information about a user's Internet activity is his Internet Service Provider (ISP).

[35] http://www.anonymizer.com/software/Fsecure.html.

[36] Freedom system 2.0 Architecture, December 18, 2000.

[37] http://www.anonymizer.com, URL Encryption FAQ.

[38] http://www.anonymizer.com/software/Fsecure.html.

[39] Freedom system 2.0 Architecture, December 18, 2000.

[40] http://www.anonymizer.com/software/Fsecure.html.

[41] Industry Canada, Le commerce électronique au Canada: Instaurer la confiance dans l'économie numérique, "Sécurité et cryptographie – Politique cadre en matière de cryptographie aux fins du comnmerce électronique, Pour une économie et une société de l'information au Canada", December 10, 2000. http://e-com.ic.gc.ca/francais/crypto/63d13.html.

[42] Directive 95/46/EC, Recital 26 of the Preamble.

[43] For the purposes of this Directive, “personal data“ means the following: “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity” according to Article 2 of Directive 95/46/EC and the “processing of personal data” means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction according to the same article.

[44] Directive 95/46/EC, Article 3 1).

[45] Data Protection Working Party (Article 29), “Privacy on the Internet – An integrated EU Approach to On-line Data Protection”, adopted on 21st November, 2000, Working Document, 5063/00/EN/FINAL, WP 37.

[46] Directive 97/66/EC, Recital 11.

[47] Directive 95/46/EC, Article 6 (1) b) and 7.

[48] *Ibid*. Article 6 a).

[49] *Ibid*. Article 6 b).

[50] *Ibid*. Article 6 c).

[51] *Ibid*. Article 6 d).

[52] Directive 97/66/EC, Article 11 1).

[53] Data Protection Working Party (Article 29) – *op. cit.*

[54] Hes, R. and Borking, J., “Privacy-enhancing technologies: the path to anonymity” (revised edition), Registratiekamer, in cooperation with the Ontario Information and Privacy Commissioner, Achtergrondstudies en Verkenningen 11, The Hague, November 1998. http://www.registratiekamer.nl.

[55] Directive 95/46/EC, Article 7 a).

[56] *Ibid*. Article 10 b).

[57] *Ibid*. Article 10 c).

[58] *Ibid*. Article 14 b).

[59] Hes, R. and J. Borking – *op. cit*., note 54.

[60] Directive 95/46/EC, Articles 16 and 17 and Directive 97/66/EC, Articles 4 and 5.

[61] Directive 1999/93/EC on December 13, 1999 on a Community framework for Electronic signatures, Official Journal of the European Communities, January 19, 2000, L 13/12 to 13/20.

[62] Freedom system 2.0 Architecture, *op. cit*., and http://www.anonymizer.com/software/Fsecure.html.

[63] http://www.anonymizer.com, URL Encryption FAQ.

[64] http://www.freedom.net/faq/privacy.html.

[65] http://www.anonymizer.com/corporate/index.shtml.

[66] http://www.anonymizer.com/docs/legal/usage_policy.shtml.

[67] *Ibid.*

[68] *Ibid.*

[69] Data Encryption Software (DES) v2.10 is a software program that provides security for files that are stored on a computer system or transmitted over phone lines. It provides security by preventing unauthorized viewing or use of any known system or hidden file of any type.
http://members.aol.com/aseone/.

[70] Industry Canada, Le commerce électronique au Canada: Données sur le commerce électronique, "Résumé de la politique du Canada en matière de cryptographie", December 10, 2000. http://e-com.ic.gc.ca/francais/fastfacts/43d7.html. And Industry Canada, Le commerce électronique au Canada: Instaurer la confiance dans l'économie numérique, "Sécurité et cryptopgraphie – Politique cadre en matière de cryptographie aux fins du commerce électronique, Pour une économie et une société de l'information au Canada", February 1998.

[71] http://cwis.kub.nl/~frw/people/koops/cls2.htm#co.

[72] Its seventeen members were Australia, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Japan, Luxemburg, The Netherlands, Norway, Portugal, Spain, Turkey, United Kingdom, and the United States. Cooperating members included Austria, Finland, Hungary, Ireland, New Zealand, Poland, Singapore, Slovakia, South Korea, Sweden, Switzerland, and Taiwan.

[73] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. http://www.acq.osd.mil/acic/treaties/wass/wassenr4.htm.

[74] *Ibid*.

[75] The Participating States of the Wassenaar Arrangement are: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovak Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and United States. http://www.wassenaar.org/docs/index1.html.

[76] The Cryptography Policy Framework for Electronic Commerce presented three policy options: i) relax controls either by matching the most liberal export policies of other countries or through recognition of the availability of similar-strength crypto products in foreign markets; ii) maintain the existing policy; and iii) extend the export controls by adding mass-market and public-domain software, possibly with a relaxation for key recovery products.

[53] Industry Canada, Le commerce électronique au Canada: Instaurer la confiance dans l'économie numérique – *op. cit*., note 41.

[78] http://strategis.ic.gc.ca/SSG/cy01156e.html.

[79] Industry Canada, Le commerce électronique au Canada: Communiqués de presse: "Le Ministre Manley présente les grandes lignes de la politique du Canada en matière de cryptographie", October 1, 1998. http://e-com.ic.gc.ca/français/releases/41d6.html.

[80] Industry Canada, Le commerce électronique au Canada: Données sur le commerce électronique, *op. cit.*

[81] Industry Canada, Le commerce électronique au Canada: Communiqués de presse – *op. cit.*

[82] *Ibid*.

[83] For more information regarding the federal government public key infrastructure, see: http://www.cio-dpi.gc.ca/pki-icp/.

[84] Industry Canada, Le commerce électronique au Canada: Communiqués de presse – *op. cit.*

[85] Export Control List. http://laws.justice.gc.ca.

[86] *Ibid*.

[87] Export and Import Permits Act, SOR/89-202. http://laws.justice.gc.ca.

[88] Mr. Lloyd Axworthy.

[89] ECL – Group 1, Category 1150: Information Security.
http://www.dfait-maeci.gc.ca/~eicb/export/gr1f_e.htm.

[90] General Export Permit No. 39 – Mass Market Cryptographic Software, Export Permits Act, SOR/99-238, June 1999, Article 2.

[91] *Ibid*. Article 3.

[92] *Ibid*.

[93] Export and Import Permits Act, Area Control List, SOR/81-543, 1999/05/12.
http://canada.justice.gc.ca/.

[94] Industry Canada, Le commerce électronique au Canada: Données sur le commerce électronique, *op. cit.*

[95] Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774.

[96] The International Traffic in Arms Regulation (ITAR) restricted export of "dual-use" cryptography (that is, cryptography that can serve both civilian and military purposes) by placing it on the Munitions List. For (relatively strong) products that can encipher information, an export license was usually issued only for use by foreign branches of American enterprises and for use by financial institutions. "Weak" cryptography (e.g., with a certain maximum key-length) could also be exported.

[97] This initiative was announced in a statement by the Vice President on October 1, 1996, and further elaborated in a November 15, 1996 executive order and memorandum, and in the Commerce Department draft Export Administration Regulations of December 30, 1996.

[98] Department of Commerce, Bureau of Export Administration, "Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List", 68572, Federal Register, Vol. 61, No. 251, December 30, 1996, Rules and Regulations.

[99] Incidentally, the Commerce Department has "borrowed" three export control and crypto specialists from the FBI and NSA to help process license applications.

[100] Department of Commerce, Bureau of Export Administration, “Revisions to Encryption Items”, 2492, Federal Register, Vol. 65, No. 10, January 14, 2000, Rules and Regulations.

[101] Department of Commerce, Bureau of Export Administration, “Encryption Items”, 50516, Federal Register, Vol. 63, No. 183, September 22, 1998, Rules and Regulations, and Department of Commerce, Bureau of Export Administration, “Encryption Items”, 72156, Federal Register, Vol. 63, No. 251. December 31, 1998, Rules and Regulations.

[102] Department of Commerce, Bureau of Export Administration, “Revisions to Encryption Items”, 2492, *op. cit*., note100.

[103] Department of Commerce, Bureau of Export Administration, “Revisions to Encryption Items”, 62600, Federal Register, Vol. 65, No. 203, October 19, 2000, Rules and Regulations, and Office of Strategic trade and foreign policy controls, Information Technology Controls Division, Commercial Encryption Export Controls, Regulations. http://www.bxa.doc.gov/Encryption/regs.htm.

[104] This restriction is now found in Department of Commerce, Bureau of Export Administration, “Revisions to Encryption Items”, 62600, Federal Register, Vol. 65, No. 203, October 19, 2000, Rules and Regulations, that clearly states that no exports without a license are authorized to these countries.

[105] Part 740.17 (b) (3) (vi),), Encryption License Exception Chart, Part 740 of the Export Administration Regulations, October 19, 2000. http://www.bxa.doc.gov/Encryption/lechart1.html.

[106] *Ibid*. Part 740.17 (b) (1).

[107] *Ibid*.

[108] These countries are Austria, Australia, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland and the United Kingdom according to Supplement 3 to Part 740, Encryption License Exception Chart, Part 740 of the Export Administration Regulations, October 19, 2000. http://www.bxa.doc.gov/Encryption/lechart1.html.

[109] Council Regulation (EC) No 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology (Official Journal L159, 30.1.2000), in force since September 29, 2000.

[110] U.S. Department of Commerce, Bureau of Export Administration, Office of Strategic Trade & Foreign Policy Controls, Information Technology Controls Division, “Encryption Fact Sheet”, October 19, 2000. http://www.bxa.docv.gov/Encryption/19Oct2Kfactsheet.html.

[111] U.S. Department of Commerce – Bureau of Export Administration, Office of Strategic Trade & Foreign Policy Controls, Information Technology Controls Division, “Encryption Policy”, October 19, 2000. http://bxa.doc.gov/Encryption/Oct2KqandAs.html.

[112] Loi 96-659 du 26 Juillet 1996 sur la réglementation des télécommunications.

[113] Loi no 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications.

[114] Décret no 98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les declarations et accordées les autorisations concernant les moyens et prestations de cryptologie (This decree restricted encryption imports into France, including those over the Internet) and Décret no 98-102 du 24 février 1998 définissant les conditions dans lesquelles sont agréés les organismes gérant pour le compte d’autrui des conventions secrètes de cryptologie en application de l’article 28 de la loi no 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications. http://www.legifrance.gouv.fr/.

[115] For example, see Décret n°98-206 du 23 mars 1998 définissant les catégories de moyens et de prestations de cryptologie dispensées de formalité préalable, and Arrêtés du 13 mars 1998 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie, Arrêté du 13 mars 1998 définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fourniture d'un moyen ou d'une prestation de cryptologie, Arrêté du 13 mars 1998 fixant la forme et le contenu du dossier de demande d'agrément des organismes gérant pour le compte d'autrui des conventions secrètes, Arrêté du 13 mars 1998 définissant le modèle de notification préalable par le fournisseur de l'identité des intermédiaires utilisés pour la fourniture de moyens ou prestations de cryptologie soumis à autorisation, Arrêté du 13 mars 1998 fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes, Arrêté du 13 mars 1998 fixant le tarif forfaitaire pour la mise en oeuvre des conventions secrètes au profit des autorités mentionnées au quatrième alinéa du II de l'article 28 de la loi 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications.

[116] R. Hes and J. Borking - *op. cit*., note 54.

[117] The Service Central de la Sécurité des Systèmes d'Information (SCSSI) is the regulatory body in France as far as cryptography is concerned. SCSSI comes under the authority of the Secretary General for National Defense (SGDN) and has a direct reporting line to the office of the Prime Minister of France.

[118] Arrêté du 13 mars 1998 fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes.

[119] Décret no 98-206 du 23 mars 1998 définissant les catégories de moyens et de prestations de cryptologie dispensées de formalité préalable.

[120] Such as video-scramblers and ATMs.

[121] Décret no 98-207 du 23 mars 1998 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.

[122] Baker, Stewart A. and Hurst, Paul R., "The Limits of Trust: Cryptography, Governments and Electronic Commerce", Kluwer Law International, The Hague, The Netherlands, 1998, p.130.

[123] Conférence de presse à l'issue du Comité Interministériel pour la société de l'information, à l'Hôtel de Matignon, le 19 janvier 1999. http://www.premier-ministre.gouv.fr/.

[124] Décret no 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable.

[125] Décret no 99-199 du 17 mars 1999 spécifiant les catégories de cryptographie requérant une déclaration.

[126] Loi no 96-659 - *op. cit*.

[127] Décret no 98-101 - *op. cit*., and Journal Officiel of February 25, 1998.

[128] Décret no 99-199 and Décret no 99-200 - *op. cit.*

[129] Décret no 99-200, Article 1.

[130] Décret no 99-200, Article 2.

[131] Décret no 99-199, Article 3 (1).

[132] Décret no 99-199 – *op. cit*.

[133] Council Regulation (EC) No 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology (Official Journal L159, 30.1.2000), in force since 29 September 2000.

[134] The December 1994 EU Council Regulation (EC) No. 3381/94 (amended by Regulation (EC) 837/95 of April 10, 1995) and EU Council Decision No. 94/942/CFSP (amended by Council Decision 98/232/CFSP and EU Council Decision 1999/193/GASP), in force since July 1995, regulated the export of dual-use goods, including cryptography.

[135] Décret no 99-200, Article 2.

[136] Décret 99-199, Article 2.

[137] http://www.afuu.fr/crypto/.

[138] *Ibid*.

[139] Directive 95/46/EC, Articles 6 and 7.

[140] Data Protection Working Party (Article 29) – *op. cit.*

[141] Hes, R. and Borking, J. – *op. cit*., note54.

[142] Directive 97/66/EC, Articles 4 and 5.

[143] Freedom system 2.0 Architecture, *op. cit*., and http://www.anonymizer.com/software/Fsecure.html.

[144] http://www.anonymizer.com, URL Encryption FAQ.

[145] Directive 95/46/EC, Articles 16, 17 and Directive 97/66/EC, Articles 4 et 5.

[146] Dr. Ulrich Sieber, University of Würzburg, "Legal Aspects of Computer-Related Crime in the Information Society", prepared for the European Commission, Version 1.0 of January 1, 1998.

[147] http://freedom.net/appendix.html.

[148] http://www.anonymizer.com/docs/legal/usage_policy.shtml.

[149] http://freedom.net/legal.html.

[150] http://www.anonymizer.com/docs/legal/agreement.shtml.

[151] http://www.anonymizer.com/irc/.

[152] In order to utilize the Anonymizer service, the user need to download a SSH program. In the United States, Data Fellows sells F-Secure Version 1 and Van Dyke Technologies sells SecureCRT both of which are compatible with the Anonymizer's service.

[153] General Export Permit No. 39 – Mass Market Cryptographic Software, Export Permits Act, SOR/99-238, June 1999, Article 3.

[154] http://www.freedom.net.

[155] This restriction is now found in Department of Commerce, Bureau of Export Administration, “Revisions to Encryption Items”, 62600, Federal Register, Vol. 65, No. 203, October 19, 2000, Rules and Regulations, that clearly states that no exports without a license are authorized to these countries.

[156] These countries are Austria, Australia, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland and the United Kingdom according to Supplement 3 to Part 740, Encryption License Exception Chart, Part 740 of the Export Administration Regulations, October 19, 2000. http://www.bxa.doc.gov/Encryption/lechart1.html.

[157] http://www.anonymizer.com/docs/legal/agreement.shtml.

[158] Part 740.17 (b) (1), Encryption License Exception Chart, Part 740 of the Export Administration Regulations, October 19, 2000. http://www.bxa.doc.gov/Encryption/lechart1.html.

[159] Décret no 99-200 – *op. cit*., Article 2.

[160] Décret no 99-199 – *op. cit*., Article 3 (1).

[161] Décret no 99-199 - *op. cit.*

[162] Council Regulation (EC) No 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology (Official Journal L159, 30.1.2000), in force since September 29, 2000.

[163] Décret 99-200 – *op. cit*., Article 2.

[164] Décret 99-199 – *op. cit*., Article 2.