# Pretty Good Privacy (PGP)

COMP516: RESEARCH METHODS IN COMPUTER SCIENCE

Assignment 1: 2,000 Word Essay

Pretty Good Privacy (PGP) is a free software tool, originally developed by Philip R. Zimmermann and now maintained by PGP Corporation, that enables people to communicate securely, even across insecure channels. It achieves this through the use of public-key cryptography technology. This essay discusses the reasons for PGP's development and explores some of the political and technical issues that have arisen as a result of its widespread adoption. The essay concludes with a reflection on PGP's impact on modern cryptography and computer usage, and a discussion of contemporary issues that are faced by both developers and users of modern cryptographic software.

Since the passing of the Omnibus Crime Control and Safe Streets Act of 1969 by the United States Congress, the law enforcement agencies of the U. S. government have viewed lawful communications interception as an invaluable tool in criminal investigation; one to only be used in exceptional circumstances and where permitted by court order. At the time the Act was passed, the majority of the international public switched telephone network was implemented using analogue technology, allowing for straightforward application of a 'wiretap' device to the physical line at the exchange. Dempsey conducts a thorough review of the effects of this law in [7].

The efficacy of physical wiretapping methods was impaired as telecommunications networks became increasingly sophisticated and complex over time. The emergence of newer communications devices, such as cellular telephones, also frustrated law enforcement agencies [9]. As a result, the early 90s saw the introduction of several Senate and House Bills proposed with the aim of modifying wiretapping law to allow for more expedient use of call recording and logging equipment (such as 'pen registers' and 'trap-and-trace devices') in investigations [16].

In an attempt to "encourage electronic communication equipment providers to design such equipment to allow law enforcement agencies […] to more easily conduct surveillance activities" [9], Senators Joseph Biden and Dennis DeConcini introduced Senate Bill 266 to the U.S Senate in January 1991 as part of the Comprehensive Counter-Terrorism Act of 1991 (CCTA) [10]. Section 2201 of the Bill contained the following:

> "It is the sense of Congress that providers of electronic communications services and the manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text content of voice, data, and other communications when appropriately authorized by law."

Identical language was also submitted as Section 545 of a second, separate piece of legislation: the Violent Crime Control Act of 1991 (VCCA) (Senate Bill 618) [11].

Proponents of Section 2201 claimed that its purpose was not to encourage the extension of the scope of existing laws beyond their current state, but to encourage the elimination of any technical barriers arising from the adoption of advancing technology. However, due to the imprecise language used, many professionals in the fields of computer science, software engineering and law observed that Section 2201, as it was worded, would have a 'chilling effect' on the research, development and use of encryption. The text does not directly refer to, or forbid, the use of encryption, yet it was noted that the phrase 'plain text content' has a specific meaning and would rarely be used outside the context of differentiation from ciphertext [19].

As an expression of the 'sense of Congress', the passage of either Bill would not give this text the status of law [12]. However, a common concern was that the passage of the Act would allow the United States government to freely introduce encryption suppression measures at a later date with little opposition, due to the Act as a precedent (see Ware in [15]).

Available archives of these discussions include the ACM Committee on Computers and Public Policy Forum on Risks to the Public in Computers and Related Systems (RISKS) [14][15], TELECOM Digest & Archives [16], and the various archives of Usenet newsgroups available on sites such as Google Groups [19].

One argument against the Bill maintained that it would require that all implementations of encryption algorithms, both hardware and software, provide a 'back door', 'master key' or equivalent measure allowing a law enforcement agency to access to the plain text content of any encrypted transmission (subject to proper process). The presence of a back door carries the risks of misuse by both internal

agents, who would then possess the ability to indiscriminately access the plain-text of any transmission without oversight, and external agents, who may compromise a back door and gain the ability to decrypt a communication without the knowledge of the participants.

A second argument contended that the Bill would require all users to submit to some measure of government administered key escrow. Two forms of key escrow were discussed in RISKS (see Leichter in [15]). In the first form, the government maintains control of the manufacture and distribution of all encryption methods and keys, reserving the ability to decrypt any encrypted message when required. In this system, permitted encryption algorithms would not allow the end-user to generate their own keys. The second form compels communicating parties to register all cryptographic protocols and keys used with the government. Key escrow measures such as these would prohibit the use of public-key encryption in communications across publicly accessible servers, as the administrators of said servers would be unable to provide the private keys necessary to decrypt the messages, these being held only by the communicating parties. Such legislation would be comparable to that established in France as part of the 'December 29, 1990' telecommunications law [32, 33]

Additional criticisms included that although the Bill appeared to be an appropriate modernisation of existing laws regarding lawful interception, it was observed that 'traditional' wiretapping of telephone communications required a direct, concerted effort on the part of the investigators whereas the implementation of the proposed laws upon a modern digital telecommunications network would allow for the uninhibited mass surveillance of the complete voice and data transmissions of considerably more citizens beyond current capabilities.

The recently formed digital civil rights organisation Electronic Frontier Foundation (EFF) actively opposed the Bill from its inception; a statement stating their opposition to the bill was published in the EFF fortnightly newsletter, EFFector Online [17]. Their activities included meetings with a number of Senators, including Biden, and the authoring of a joint 'Statement in Support of Communications Privacy' [18] with a large number of industry professionals.

It was these issues that led Philip Zimmermann, a software engineer and political activist, to release the first version of Pretty Good Privacy (PGP) for MS-DOS in June 1991. The software was released electronically on Usenet on June 5th, and made available at no charge [21].

In 1986, Zimmermann began the development of the software basis for what would later become PGP, with the intention of using it for the development of commercial products. His initial work included a paper outlining the need for a standardised data format protocol for public-key cryptography, with a view to promoting the adoption of public-key cryptography in commercial applications [20].

It was in December 1990 that Zimmermann, as a response to what he perceived as increasing aggression toward personal privacy in U.S. government policy, changed his attention to the application of PGP as a political tool. In the original PGP User's Guide [22], Zimmermann gives his rationale for developing PGP, stating that if the use of encryption were to become widespread in the public, then it would be more difficult for the U.S. government to attempt to criminalise it at a later date. He also maintained that a strong, freely available cryptography tool would be of great aid to those who have a critical need for it, such as political activists and dissidents, wherever they may be in the world.

PGP was not the only publicly available software suite using public-key cryptography, as Zimmermann noted in his 1986 paper [20], yet it was perhaps the first to use telecommunications networks (such as Usenet, the WELL, BIX, FidoNet and CompuServe) and word-of-mouth as its primary methods of distribution and dissemination, a method Zimmermann refers to as 'guerrilla-ware'. It may have also been the first complete end-user cryptographic tool to offer its source code freely for public peer review, outside of the context of academia. In the PGP User's Guide [22], 'Beware of Snake Oil', Zimmermann expresses criticism on the quality of certain cryptographic applications available at the time, specifically in their use of proprietary and undocumented encryption algorithms, asserting that a trustworthy cryptography application would be built upon peer reviewed cryptographic techniques.

In [31], Zimmermann recalls that he had little direct influence on the initial distribution of PGP. It was his intention that the program only be made available for

distribution within the U. S., yet the liberal copyleft terms under which PGP was released enabled its users to electronically redistribute the software freely around the world. Due to its ready availability, zero cost, and its 'hacker' reputation, PGP rapidly became popular throughout the electronic world. Just days after the initial release, Zimmermann was receiving many offers of support and thanks from eager users. With the assistance of a team of volunteer software engineers, version 2.0 of PGP was released in September 1992. The popularity of this new piece of software did not escape the notice of the U. S. government.

In September 1993, it was reported that Zimmermann had become the target of a U.S. government criminal investigation into possible violations of the International Traffic in Arms Regulations (ITAR) code [24]. These regulations forbid the export of cryptographic technology from the U. S. where the size of the key used in the algorithm exceeds 40 bits, classing them as 'munitions'. PGP uses keys of size 128 bits. Two companies interested in producing commercial products related to PGP were also subject to investigation. Zimmermann received support from many legal and security professionals during this investigation, including the EFF, the Electronic Privacy Information Center (EPIC) and the Computer Professionals for Social Responsibility (CPSR).

In response to the investigation, Zimmermann published the complete source code to the PGP software through the MIT Press in the form of a hardback book entitled 'PGP Source Code and Internals' [26]. It was intended that if the book were to be unbound and the pages scanned and analysed by optical character recognition software, it would be possible to reproduce the original source files necessary to compile the software: the software would therefore be available worldwide. This is significant, as it was argued that the export of books was protected under the First Amendment. This assertion was never tested in court with respect to PGP. A similar case was contested by Phil Karn, regarding Bruce Schneier's book 'Applied Cryptography', in an attempt to force a ruling on the issue of cryptography code export [27]. In documents relating to Karn's case, a declaration from Zimmermann states that the NSA recommended that 'PGP Source Code and Internals' be subject to ITAR controls, whereas the Department of Commerce recommended otherwise [28]. The investigation into Zimmermann regarding PGP was closed without prosecution in January 1996 [29].

PGP 1.0 used a combination of related algorithms to allow for the establishment of a secure communications channel: RSA public-key encryption, the Bass-O-Matic symmetric encryption, the MD4 message digest algorithm and the MPILIB high-precision integer library.

The Bass-O-Matic symmetric encryption cipher was a unique algorithm designed by Zimmermann specifically for PGP. From discussions with cryptographer Eli Biham in 1991, Zimmermann learned of a number of serious vulnerabilities in the Bass-O-Matic algorithm leading to the adoption of IDEA as the symmetric algorithm in subsequent versions of PGP.

There were also issues with the use of RSA public-key cryptography with MPILIB, as RSA Data Security Inc. held a patent on the RSA algorithm at the time of PGP's release. The original PGP documentation strictly indicates that the user is responsible for ensuring that they are correctly licensed for their use of RSA, but this was insufficient for RSA Data Security Inc., which threatened legal action. An agreement was later reached whereby Zimmerman would cease distribution of PGP. Active development of PGP was relocated to Europe, with Zimmermann in an advisory role.

Version 2.5 of PGP was prepared using a compatible, alternative high-precision integer library, RSAREF, produced by RSA Data Security Inc... With this library in place of MPILIB, users were permitted to use RSA without a license for non-commercial or personal use only. Zimmermann agreed for MIT to act as the official distributor of this new version of PGP in the U. S...

The originators of RSA were only able to secure a patent for the algorithm in the U. S... As a result, the RSA algorithm could be freely used by anyone outside of the U. S., but the RSAREF library could not legally be exported due to ITAR controls. This disparity meant that as of 1994, there were two different, albeit compatible, versions of PGP being maintained by the community: PGP 2.6 in the U. S. using RSAREF, and PGP 2.6i (international) elsewhere using MPILIB. This situation was resolved when RSA Data Security Inc. released the patent on RSA into the public domain in September 2000. To avoid any such problems in the future, PGP Version 3 was developed specifically with a focus on the use of non-patented

algorithms: the CAST-128 symmetric key algorithm and the DSA and ElGamal asymmetric key algorithms.

After the investigation had closed, Zimmermann and his team formed a new company, PGP Incorporated, to develop commercial products based upon PGP. In 1997, PGP Inc. proposed OpenPGP, an open standard based on PGP, to the Internet Engineering Task Force (IETF). This open standard allowed for the independent development of PGP compatible applications, including 'GNU Privacy Guard' released under the GNU Public License by the Free Software Foundation.

PGP Inc. was later bought by Network Associates Inc. in 1997. In 2001, PGP Corporation, a newly formed company of ex-PGP team members purchased the PGP intellectual property from Network Associates. PGP Corporation continues to support and develop PGP software security products, with Zimmermann acting as a special advisor and consultant.

Privacy issues remain relevant today as the governments of the world continue to adjust to changes in global telecommunications infrastructure. Similar legislation to that pursued by the U. S. government agencies in the 90s appears frequently in many countries, with regards to the suppression of private cryptography, the introduction of measures such as mandatory key escrow or the enabling of mass surveillance over the Internet. Civil rights campaigners and societies such as the EFF continue to campaign against these issues and their chilling effects on innovation. A full discussion on modern privacy issues with respect to wiretapping and cryptography, led by cryptography specialist Whitfield Diffie, can be found in the latest 'Communications of the ACM' [34].

In the U. K., Part III of the Regulation of Investigatory Powers Act (RIPA) 2000 compels citizens to make their encryption keys available when served with a section 49 notice during an investigation. Non-compliance is a criminal offence punishable by a jail sentence. In August 2009, two people were convicted of withholding encryption keys [35]. Civil rights groups are concerned that this measure may be used to covertly criminalise encryption.

# REFERENCES


[1] Mollin, A. R. (2003) *RSA and Public-Key Cryptography*, Chapman & Hall/CRC.

[2] Konheim, A. G. (1981) *Cryptography: A Primer*, John Wiley & Sons.

[3] Beckett, B. (1988) *Introduction to Cryptology*, Blackwell Scientific Publications.

[4] Lucas, M. W. (2006) *PGP & GPG – Email for the Practical Paranoid*, No Starch Press.

[5] Van Tilborg, H. C. A. (2005) *Encyclopedia of Cryptography and Security*, Springer.

[6] Schneier, B. (2000) *Secrets & Lies: Digital Security in a Networked World*, John Wiley & Sons.

[7] Dempsey, J. X. (1997) *Communications Privacy in the Digital Age: Revitalising the Federal Wiretap Laws to Enhance Privacy*, Albany Law Journal of Science and Technology, Volume 8, Number 1. (Available at: http://www.cdt.org/ publications/lawreview/1997albany.shtml, accessed 8th October 2009)

[8] Neugent, B. (1992) *Encryption: A Few Cryptic Remarks*, ACM SIGSAC Review, Volume 10, Issue 1, Pages: 29 – 36, ACM.

[9] United States Senate (1991) *Description of Section 2201: Cooperation of Telecommunications Providers With Law Enforcement*, Congressional Record 137 Cong. Rec. S1159-03, U.S. Library of Congress. (Archived at: http://w2.eff.org/Legislation/Bills_by_sponsor/Old/biden_s266_91.comments, accessed 15th October 2009)

[10] United States Senate (1991) *Comprehensive Counter-Terrorism Act of 1991*, Subtitle B: Electronic Communications: Section 2201, Cooperation Of Telecommunications Providers With Law Enforcement, U.S. Library of Congress. (Available at: http://thomas.loc.gov/cgi-bin/bdquery/ z?d102:s.00266: , accessed 15th October 2009)

[11] United States Senate (1991) *Violent Crime Control Act of 1991*, Subtitle B: Preventing Domestic and International Terrorist Acts, Part II: Electronic Communications, Cooperation Of Telecommunications Providers With Law Enforcement, U.S. Library of Congress. (Available at: http://thomas.loc.gov/cgi-bin/bdquery/z?d102:s.00618: , accessed 15th October 2009)

[12] Davis, C. M. (2007) *"Sense of" Resolutions and Provisions*, CRS Report for Congress, Congressional Research Service, U.S. Library of Congress.

[13] Cohen, N. (1994) *Wiretapping and the Digital Telephony Bill: Past and Present*. (Available at: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall94-papers/cohen-digital-telephony.html, accessed 15th October 2009)

[14] Murray, W. H. (1991) *Re: U.S. Senate 266, Section 2201 (Cryptographics)*, 10th April 1991, The Risks Digest Volume 11: Issue 43, Forum on Risks to the Public in Computers and Related Systems, ACM Committee on Computers and Public Policy. (Available at: http://catless.ncl.ac.uk/Risks/11.43.html#subj1, accessed 15th October 2009)

[15] RISKS Contributors (1991) *Re: U.S. Senate 266, Section 2201 (Cryptographics)*, 11th April 1991, The Risks Digest Volume 11: Issue 44, Forum on the Risks to the Public in Computers and Related Systems, ACM Committee on Computers and Public Policy. (Available at: http://catless.ncl.ac.uk/Risks/11.44.html, accessed 15th October 2009)

[16] Marshall, P. (1991) *Electronic Surveillance Bill in WA; Electronic Communications*, 4th February 1991, TELECOM Digest Volume 11, Issue 51, TELECOM Digest & Archives. (Available at: http://massis.lcs.mit.edu/archives/back.issues/1991.volume.11/vol11.iss051-100, accessed 15th October 2009)

[17] Electronic Frontier Foundation (1991) *EFF Opposes Federal Restriction on Encryption Use*, EFFector Online, Volume I, Issue 5, May 1991, Van der Leun, G., Godwin, M., Kapor, M., (Editors), Electronic Frontier Foundation. (Available at: http://w2.eff.org/effector/effect01.05, accessed 15th October 2009)

[18] Kapor, M. et al (1991) *Statement in Support of Communications Privacy*, 10th June 1991, Electronic Frontier Foundation, Computer Professionals for Social Responsibility, RSA Data Security Inc., (Available at: http://catless.ncl.ac.uk/Risks/12.01.html#subj5, accessed 16th October 2009)

[19] Riddle, M. H. (1991) *Re: You're All A Bunch of Terrorists*, 9th May 1991, comp.dcom.telecom newsgroup. (Available at: http://preview.tinyurl.com/1991-05-09-cryptography-1/, accessed 16th October 2009)

[20] Zimmermann, P. R. (1986) *A Proposed Standard Format for RSA Cryptosystems*, IEEE COMPUTER, Volume 19, Issue 9, Pages 21 – 34, IEEE Computer Society.

[21] Zimmermann, P. R. (1991) *Public Key Crypto Freeware Protects E-MAIL*, 7th June 1991, The Risks Digest Volume 11: Issue 86, Forum on Risks to the Public in Computers and Related Systems, ACM Committee on Computers and Public Policy. (Available at: http://catless.ncl.ac.uk/Risks/11.86.html#subj3, accessed 11th October 2009)

[22] Zimmermann, P. R. (1991) *PGP User's Guide*, 5th June 1991, Version 1.0, Phil's Pretty Good Software.

[23] Markoff, J. (1991) *Move on Unscrambling Of Messages Is Assailed*, 17th April 1991, Section A, Page 16, New York Times. (Available at: http://www.mytimes.com/1991/04/17/business/move-on-unscrambling-of-messages-is-assailed.html, accessed 14th October 2009)

[24] Detweiler, L. (1993) *ITAR Issues in PGP & Moby Crypto Subpoenas*, The Risks Digest Volume 15: Issue 11, Forum on the Risks to the Public in Computers and Related Systems, ACM Committee on Computers and Public Policy. (Available at: http://catless.ncl.ac.uk/Risks/15.11.html#subj3, accessed 15th October 2009)

[25] Lebkowsky, J. (1993) *An Interview with Phil Zimmermann, Creator of PGP*, The Internet Code Ring!. (Available at: http://www.well.com/gopher/hacking/pgp.up, accessed 16th October 2009)

[26] Zimmermann, P. R. (1995) *PGP Source Code and Internals*, MIT Press.

[27] Karn, P. (2002) *The Applied Cryptography Case*, www.ka9q.net. (Available at: http://www.ka9q.net/export/, accessed 20th October 2009)

[28] Zimmermann, P. R. (1995) *Declaration of Philip R. Zimmermann in Support of Plaintiffs' Opposition to Defendants' Motion to Dismiss*, United States District Court for The District of Columbia.

[29] Dubois, P. L. (1996) *Significant Moments in PGP's History: Zimmermann Case Dropped*, www.philzimmermann.com. (Available at: http://www.philzimmermann.com/EN/faq/index.html, accessed 16th October 2009)

[30] Back, A. (1999) *PGP Timeline*, www.cypherspace.org. (Available at: http://www.cypherspace.org/adam/timeline/, accessed 13th October 2009)

[31] Zimmermann, P. R. (2001) *PGP Marks 10th Anniversary*, www.philzimmermann.com (Available at: http://www.philzimmermann.com/EN/news/PGP_10thAnniversary.html, accessed 20th October 2009)

[32] Koops, B. (1996) *A Survey of Cryptography Laws and Regulations*, The Computer Law & Security Report, November – December 1996, pages 349 – 355. (Available at: http://rechten.uvt.nl/koops/CLSR-CLS.HTM, accessed 16th October 2009)

[33] Oram, A. (1998) *France Fails to Decipher The Path to Encryption*, The American Reporter. (Available at: http://praxagora.com/andyo/ar/crypto_model.html, accessed 16th October 2009)

[34] Diffie, W., Landau, S. (2009) *Communications Surveillance: Privacy and Security at Risk*, Communications of the ACM, Volume 52, No. 11, Pages 42 – 47.

[35] Williams, C. (2009) *Two Convicted for Refusal to Decrypt Data*, The Register. (Available at: http://www.theregister.co.uk/2009/08/11/ripa_iii_figures/, accessed 20th October 2009)