State Access and Regulation of Encryption Codes

1. ARTICLES

1.1 A. Colangelo & A. Maurushat, Exploring the Limits of Computer Code as a Protected Form of Expression: A Suggested Approach to Encryption, Computer Viruses and Technological Protection Measures, (McGill Journal of Law vol. 51, p. 47, 2005-2006)

This article uses a comparative study of free speech protection in the U.S. and Canada to study the restrictions on encryption, viruses and other technologies. Following a detailed discussion of the U.S. cases of *Bernstein* v. *the United States (Department of Justice)*, *Karn* v. *the United States (Department of Justice)* and *Junger* v. *Daley*, it applies the *Oakes* test to the Export and Import Permits Act, 1985 of Canada in light of the Wassenaar Agreement to test the validity of the Canadian regulations.

1.2 Anon. note, Bernstein, Karn and Junger: Constitutional Challenges to Cryptographic Regulations (Alabama Law Review, vol. 50, no. 3, p. 869, 1999-2000)

While growth of communications technologies opens up greater avenues to exercise free speech rights, governmental restrictions (such as export regulations and interception laws) on grounds,

inter alia, of national security pose threats to such exercise by blocking whole areas of communication. The article argues that such regulations must be declared unconstitutional by drawing upon elaborate discussion of the decisions in *Bernstein, Karn* and *Junger*. Additionally, the article looks at implications for the Fourth and Fifth Amendments, and at contemporary legislative attempts to address these issues. A preliminary overview of encryption technologies is also provided.

1.3 C. Crump, Data Retention: Privacy, Anonymity and Accountability Online (Stanford Law Review, vol. 56, no. 1, p. 191, 2003)

This article looks broadly at the implications of data retention, and does not focus specifically on encryption. In addition to elaborately considering the privacy implications of data retention, it argues that data retention eliminates all possibility of anonymous speech (as a violation of the First Amendment to give and receive information and associate anonymously). It seeks to balance the value of near-perfect anonymity on the Internet with the need for accountability that arises from security concerns.

1. 4 C. Kuner, Legal Aspects of Encryption on the Internet (International Business Law, vol. 24, p. 186, 1996)

This note provides a basic understanding of encryption technologies and the corresponding legal regulations. Along with brief descriptions of legislative control of encryption technology in the U.S., the E.U. and Russia & Belarus, it also analyses the implications of such control. While the laws discussed in this note are largely obsolete, given legislative and policy advances, it prepares the reader to appreciate nuances of the encryption debate.

1.5 Comment, Cryptobabble: How Encryption Export Debates are Shaping Free Speech for the New Millennium (North Carolina Journal of International Law and Commercial Regulation, vol. 24, p. 125, 1998-1999)

This comment is a comprehensive approach to the encryption debate in light of its First Amendment implications. Apart from considering the evolution of cryptographic technology and evaluating its benefits (technology v. security), it analyses the legal regulations in light of the three cases previously referred to. In the context of existing tests, it considers issues of prior restraint, overbreadth of rstrictions and privacy. Encryption policies from different jurisdictions

are compared with that of the U.S., along with a detailed discussion on balancing national security with privacy.

1.6 Comment, Privacy and Encryption in Cyberspace: First Amendment Challenges to ITAR, EAR and their Successors (San Diego Law Review, vol. 34, p. 1401, 1997)

This Comment is a detailed discussion on government policy on encryption over the past two decades. Beginning with a brief tutorial on encryption technology, it goes on to analyse the Clinton administration's encryption export controls aimed at discouraging the spread of strong crypto. It then looks at the judicial review of such regulations, surveying three decisions on the First Amendment implications of encryption codes. It delves deeper into the justifiability of such regulations, in light of judicial standards of prior restraint (addressed in detail in light of countervailing security concerns), with specific reference to the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) regimes.

1.7 D.H. Kaye, The Propriety of Facial Challenges to the Use of Prior Restraints on the Internet (Jurismetrics, vol. 40, p. 445, 1999-2000)

This paper is primarily procedural, but initially considers the then-existing position of law (federal court rulings in *Junger*, etc.) on the issue of whether encryption source codes fall within First Amendment protection as scientific speech. Its focus, however, is on the standing of litigants in court to facially challenge an encryption export regulation requiring persons to have a licence as unconstitutional, when they have not applied for such a licence. It concludes that this reason should not prevent a successful challenge.

1.8 G. Gordon, Breaking the Code: What Encryption Means for the First Amendment and Human Rights (Columbia Human Rights Law Review, vol. 32, p. 477, 2000-2001)

This article studies contemporary issues associated with encryption vis-à-vis the First Amendment. In light of the (now largely replaced) Export Administration Regulations in the U.S. and the cases of *Bernstein*, *Junger* and *Karn*, Gordon analyses whether First Amendment protection for encryption exists at the following levels: the source code itself (argument: may represent speech insofar as it consists of mathematical ideas), the scrambled speech (argument: process of encryption may be considered expressive speech), and against compelled disclosure

(extension of constitutional protection against forced disclosure of sensitive information without compelling governmental interest).

1.9 J. Terence Stender, Too Many Secrets: Challenges to the Control of Strong Crypto and the National Security Perspective (Case Western Reserve Journal of International Law, vol. 30, p. 287, 1998)

A comprehensive take on crypto control regimes in the U.S., this article considers the rights v. security debate in great detail, and analyses existing and past regulations (the ITAR and EAR) for the ideal balance. Inevitably, absolute proscription of regulation is concluded to be impossible; however, it advocates a via-media for encryption regulation: the key escrow control of encryption.

1.10 J. C. Mandelman, Encrypting the Constitution: To Speak, Search and Seize in Cyberspace, Albany Law Environmental Outlook Journal, vol. 8, p. 227, 1997-1998).

This article considers the question of First Amendment implications on encryption code and their restriction elaborately. It addresses the following questions: is encryption source code speech? Does regulation of encryption export violate the First Amendment? Concerns about the chilling effects of such regulation and of compelled disclosure are considered. Additionally, Fourth and Fifth Amendment implications are considered, as are benefits and harms of key escrow.

1.11 K. A. Moerke, Free Speech to a Machine? Encryption Software Source Code is Not Constitutionally Protected "Speech" Under the First Amendment, Minnesota Law Review, vol. 84, p. 1007, 1999-2000)

Following conflicting decisions in *Bernstein*, *Karn* and *Junger*, Moerke considers the various arguments in favour of and opposing the protection of encryption source code under the First Amendment. Identifying that this will affect export regulations, she traces free speech standards in the U.S. and the nature and development of encryption source code, before concluding that while the source code itself may not be protected under the First Amendment, it may be eligible for some protection as it protects the ability to speak privately.

1.12 M. P. Voors, Encryption Regulation in the Wake of 9/11: Must We Protect National Security at the Expense of Autonomy?, Federal Communications Law Journal, vol.55, p. 331, 2002-2003)

Voors is of the view that encryption regulation had, in the decade preceding 9/11, been dominated by privacy concerns and the need to ensure a competitive edge in the national and international markets for domestic developers. This had resulted in relaxed export controls, and lesser power to governmental agencies to intercept encrypted communication. Voors considers that controls instituted following 9/11 prioritised national security at the expense of privacy and economic interests. He advocates the adoption of the Magic Lantern, the F.B.I.'s new software, as a method to ideally balance these competing interests.

1.13 Note, Redefining National Security in the Technology Age: The Encryption Export Debate (Journal of Legislation, vol. 26, p. 337, 2000)

This note traces the development of encryption technologies in the United States, and the changing legislative controls on the same, ranging from D.E.S., R.S.A. and D.S.S. to E.A.R. and the Wassenaar Agreement. The primary focus, however, is on analysing the need to balance competitive edge in encryption exports with national security interests. It looks to this end at the N.S.A.'s involvement in software development.

1.14 Note, Freedom to Speak Unintelligibly: The First Amendment Implications of Government-Controlled Encryption, William and Mary Bill of Rights Journal, vol. 4, p. 1165, 1995-1996)

This note follows encryption regulation through the Clinton administration, explaining details of the Escrowed Encryption Standard, and opposition to it on the grounds of privacy, effectiveness and economic viability. Constitutional challenges to mandatory encryption regulation is discussed extensively: Fourth and Fifth Amendment concerns are briefly discussed. Regarding the First Amendment, the Note considers, *inter alia*, freedom of association, freedom of expression (with specific attention to media), and the distinction between content-neutral and content-based restrictions. It further lays down and analyses the test to determine constitutionality of encryption restrictions.

1.15 R. Post, Encryption Source Code and the First Amendment (Berkley Technology Law Review, vol.15, p.713, 2000)

This article tackles the question of whether encryption source code is constitutionally protected. It argues that in order to determine whether source code is protected, one must necessarily take

into account the social context in which such expression is made. It first describes the scope of First Amendment protection, and seeks to fit encryption source into the same.

1.16 Z. M. Vedder-Brown, Government Regulation of Encryption: The Entry of "Big Brother" or Status Quo?, American Criminal Law Review, vol. 35, p. 1387, 1997-1998)

This article traces the encryption debate from the Clinton administration's Clipper Chip proposal, and explores the role of governmental agencies in encryption-regulation, ranging from export regulation to restrictions on purchasing power. The focus of this paper, however, is on the impact of encryption regulation on privacy and towards this end, it distinguishes between the narrow constitutional guarantee of the *right of privacy* and the wide ambit of *privacy* itself (which includes one's right to control the flow of information about oneself). In ascertaining whether the whether First Amendment protection would extend to encryption, the language metaphor ("encrypted speech resembles a foreign language") is analysed to reach the conclusion that mandatory key-recovery is a content-neutral form of speech-regulation.