

DISCUSSING THE CONSTITUTIONALITY OF REGULATING THE EXPORT OF ENCRYPTION PRODUCTS

*David Goldstone**

Good afternoon. My name is David Goldstone. As I was introduced, I am an attorney at the Department of Justice, in the Computer Crime and Intellectual Property Section. However, for the last six months, I have been working at the U.S. Attorney's Office in the Eastern District of Virginia. Therefore, I am not as up to date on the latest issues relating to encryption as I might be; so today I am only going to be speaking in my individual capacity. My views do not necessarily represent those of the Department of Justice.

Having said that, it is a pleasure to be here and a pleasure to have heard Professor Froomkin's careful analysis of the Department of Justice's FAQ (frequently asked questions) and answers on encryption.¹ It was helpful, really, to hear how much of what he saw in the FAQ he agreed with. From what I heard, if I understood him correctly, his primary concern was whether source code is or is not protected speech; his second major theme was whether we should have a "New Privacy" or whether we should confine ourselves to the old privacy that, up until now, has been the law of the land. From what I understood today, he was advocating a "New Privacy."² I would certainly encourage him to develop theories like that. I am not familiar enough, perhaps, with his theories, but I would note that a lot of the concerns that he raised—facial recognition in poor neighborhoods in England,

* Trial Attorney, U.S. Department of Justice, Computer Crimes and Intellectual Property Section; Adjunct Professor, Georgetown University Law Center; Adjunct Professor, George Washington University Law School; J.D., 1994, Harvard Law School; M.S., 1991, B.S., 1991, Massachusetts Institute of Technology. The views expressed in this speech are those of the author and do not necessarily represent the views of the United States.

1. See *Department of Justice FAQ on Encryption Policy*, U.S. DEPARTMENT OF JUSTICE (last modified Sept. 17, 1999) <<http://www.usdoj.gov/criminal/cybercrime/crypto.html>> (discussing general policy, law enforcement, and constitutional issues related to encryption).

2. See A. Michael Froomkin, *The Constitution and Encryption Regulation: Do We Need a "New Privacy"?*, 3 N.Y.U. J. LEGIS. & PUB. POL'Y 25, 34 (1999) (declaring "new privacy" fundamental to reclaiming ownership of personal facts).

tracking on highways,³ while interesting, are not the subject of my discussion: the export regulations that apply to encryption and the constitutionality thereof.⁴

I would like to review some of the constitutional arguments and criticisms. While these issues may implicate some policy positions, I would like to try to stick to the constitutional issues, not only because they are the focus of this panel, but also because in a law school setting such as this it is important to practice applying legal regimes. One of the most exciting aspects of today's discussion—for student, practitioner, and policy-maker alike—is that it provides a chance to take legal regimes with which you have become familiar in law school and apply them in a new context.

Now, there are a number of specific criticisms that are brought against the cryptography regulations: They violate the Fourth Amendment right of privacy; they violate the Fifth Amendment right against self-incrimination; and they violate the First Amendment right to free speech. We will address each of these criticisms in turn; but first, I will address a more general criticism, which I think is really a rational basis attack.

As you know, any statute, any law, must have a rational basis.⁵ What some people think is the strongest criticism of the encryption regulations has nothing to do with the Bill of Rights. Some scholars claim, "These regulations simply are not rational. They are futile. Encryption remains available overseas, and can be obtained through the Internet. The Internet makes the law useless."⁶

Now, this is a very odd argument. First of all, we do not ever expect law to be 100 percent effective. We have laws against murder and yet we know people get murdered. The idea is that the law will provide a substantial deterrent, not a perfect deterrent. So the idea that, potentially, encryption products might be available overseas, for instance, is not ordinarily a regulator's primary concern. For example, you may tell me that there is a Web site in Denmark where anyone can

3. See *id.* at 36.

4. See, e.g., Export Administration Regulations, 15 C.F.R. § 730 (1999).

5. See, e.g., *Kadrmas v. Dickinson Pub. Sch.*, 487 U.S. 450, 457-58 (1988), and cases cited therein.

6. See, e.g., Eric B. Easton, *Closing the Barn Door After the Genie is out of the Bag: Recognizing a "Futility Principle" in First Amendment Jurisprudence*, 45 DEPAUL L. REV. 1, 60 (1995) (applying "futility principle" to government's restriction on diskette distribution of source code already available via download). See also, e.g., David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1372 (1996) (arguing that "efforts to control the electronic flow of information across physical borders . . . are likely to prove futile").

download something said to be ultra-strong unrecoverable encryption software; maybe for all I know, it is simply no good or contains a Trojan Horse or some other catch; maybe, you will prove to me it does not contain a Trojan Horse by showing me the source code; then, if I am an expert computer programmer, maybe I can read the source code and figure out that the program does not contain malicious code. This extremely contingent scenario is not the regulator's primary concern. The regulator's primary concern is based on predictable, pervasive patterns, such as the following scenario: Let us say that Microsoft is going to put unrecoverable encryption software in Windows 2000 as an automatic feature; then we may likely see use of encryption go from 2 percent to 98 percent overnight. How can law enforcement be effective in an encrypted world? The law should be concerned not with the exceptions, but with the norm. The law cannot expect perfect compliance, but it can expect substantial deterrence.

What is interesting academically about this "futility" argument is how commonly it arises in the context of cyberspace. Whenever you see a case of first impression on the regulation of cyberspace, one common initial reaction is "Stop trying to regulate the Internet; regulation is hopeless." For instance, there are some proposals about Internet gambling because in many places, including New York, it is illegal to have a casino, and you cannot simply walk down and open up a casino here on West 3rd Street.⁷ Meanwhile, of course, there are Web sites that are, effectively, casinos,⁸ and some people who advertise and promote their sports betting operations to United States customers through Internet Web sites have faced civil and criminal charges.⁹ The U.S. Attorney's Office for the Southern District of New York here in Manhattan has charged them.¹⁰ When the topic of regulation arises, some people in the Internet gaming debate insist, "It is futile to try to stop Internet gaming because people will go offshore

7. See N.Y. PENAL LAW § 225 (McKinney 1999).

8. See, e.g., *RGT Links*, ROLLING GOOD TIMES ONLINE, INC. (visited Sept. 26, 1999) <<http://www.rgtonline.com/links/casinos/canoresults.cfm>> (providing links to more than 200 Internet gambling sites located around world).

9. See, e.g., *Missouri v. Coeur D'Alene Tribe*, 164 F.3d 1102, 1108-09 (8th Cir. 1999) (involving action brought by Missouri Attorney General against Native American tribe which hosted Internet gambling service from reservation in Idaho); *State by Humphrey v. Granite Gate Resorts, Inc.*, 568 N.W.2d 715, 718-21 (Minn. App. 1997) (involving complaint brought by Minnesota Attorney General against Belizian corporation hosting Internet gambling site).

10. See United States Attorney for the Southern District of New York, *Press Release*, U.S. DEPARTMENT OF JUSTICE (Mar. 26, 1998), <<http://www.usdoj.gov/criminal/cybercrime/nypr.htm>> (announcing filing of charges against owners and employees of Caribbean based Internet sports betting companies).

and set up gaming web sites there.”¹¹ But, that argument does not make it irrational to prosecute those who are clearly violating the law domestically.

This argument was also made with regard to Internet pornographic communications. There was a law known as the Communications Decency Act,¹² which intended to protect minors from indecent material. Again, people said, “How can you even try to regulate pornography on the Internet? Such regulation is futile because even if we can regulate Americans, people can provide pornography from abroad. The Internet makes legal regulation pointless.”¹³ This specific argument was presented in *Reno v. ACLU*,¹⁴ where the Supreme Court struck down the Communications Decency Act, 7-2, on First Amendment grounds.¹⁵ But, at oral argument, when this international futility argument was presented, the Justices were skeptical. They said, “Are you telling us that this law will have no effect? Are you telling us that the United States will not achieve anything by passing this law?” The argument offered was that the law would be ineffective because, although 50 percent of the indecent material was coming from the United States, the other 50 percent was from abroad. The Court responded sharply, “Are you telling us that 50 percent would not be a good start?”¹⁶ Notably, the majority opinion itself did not even raise

11. See Richard T. Pienciak, *Gambling Online a Dicey Biz, Parlaying Internet bets into a market worth millions*, DAILY NEWS (New York), Oct. 12, 1997, at 6; Michael P. Kailus, *Latest Odds On Legality Of Online Gambling*, THE INTERNET NEWSL.: LEGAL & BUS. ASPECTS, Apr. 1999, at 3.

12. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (codified as amended in scattered sections of 47 U.S.C. and declared unconstitutional by *Reno v. ACLU*, 521 U.S. 844 (1997)).

13. See, e.g., Brief for Appellees at 17-18, *Reno v. ACLU*, 521 U.S. 844 (1997) (No. 96-511), available in No. 96-511, 1997 WL 74378, at *17-18 (Feb. 20, 1997).

14. 521 U.S. 844 (1997).

15. See *id.* at 849.

16. Specifically, Justice Scalia asked, if the government “succeeds in excluding children from 250 out of 500 [indecent bookstores], that’s no use?” United States Supreme Court Official Transcript at 53, *Reno v. ACLU*, 521 U.S. 844 (1997) (No. 96-511), available in No. 96-511, 1997 WL 136253, at *53 (Mar. 19, 1997). After a colloquy with counsel regarding application of the statute extra-territorially and the extraterritorial reach of the statute, Justice Scalia observed “I don’t know that we’ve ever had a case in which it has been asserted that the difference between the constitutionality and unconstitutionality of the statute is whether it is extraterritorial. I think if the only way to make it constitutional is to interpret it as being extraterritorial, I’m not sure that we wouldn’t say, well . . . if that’s your only argument, . . . I think it’s a pretty weak argument.” *Id.* at *57.

After a colloquy with Justice Ginsburg about the speech regulations of other nations, unidentified Justices noted, with concurrence from counsel, that no “global principle” would require the United States to “let obscenity in.” See *id.* at *59. Justice Kennedy stated that “it’s a weak argument to say that the United States, if it has a

this international futility argument, nor did the concurrence or dissent.¹⁷

In addition to making “a good start” for our own enforcement, if the United States were to pass a law in the indecency context, in the gaming context, or in the cryptography context, such a law would better enable the United States to work with other countries as a leader. Because the United States is at the forefront of many legal and policy issues, it can lead on policy, especially in high-tech areas. The United States happens to be one of the most important countries for setting policy, both because of its market for the sale and use of high-tech products, and because of its software industry, where the same products are developed and produced. It would not be irrational for the United States to take the lead in international policy making, since Americans play such an important role at both ends of the high-tech economy.¹⁸

There is one notable area where the technology community does not make an argument that regulation is futile. This very interesting exception is made in the intellectual property context. Industry is continually advocating—and I think rightly so—for strong intellectual property laws in this country.¹⁹ You never hear the technological community saying, “Well, strong domestic intellectual property laws are futile because people could copy things in other countries.” Eve-

strong public policy, cannot lead the way, and maybe other nations would follow [This argument] is not your strongest argument.” *Id.*

17. *See Reno*, 521 U.S. at 844.

18. Indeed, based on its experience and expertise, the United States Department of Justice has taken a leadership role in identifying the international dimensions of crimes in cyberspace and in working with other nations to address them. *See* David Goldstone & Betty-Ellen Shave, *International Dimensions of Crimes in Cyberspace*, 22 *FORDHAM INT'L L.J.* 1924, 1927-30 (1999) (describing international computer crime cases in which U.S. Department of Justice agencies cooperated with foreign authorities). *See also* Michael A. Sussmann, *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium*, 9 *DUKE J. COMP. & INT'L L.* 451, 476 (1999) (advocating “international training and sharing of information and forensic tools” to help combat cross-border computer crime).

19. *See, e.g., Copyright Piracy on the Internet: Hearings on H.R. 2265 Before the Courts and Intellectual Property Subcomm. of the House Comm. on the Judiciary*, 105th Cong. 37 (1997) (testimony of Brad Smith, Associate General Counsel, Microsoft Corporation), available in 1997 WL 566030 (F.D.C.H.) (advocating passage of new law to punish copyright infringement via Internet regardless of defendant’s lack of commercial advantage); *Copyright Piracy on the Internet: Hearings on H.R. 2265 Before the Courts and Intellectual Property Subcomm. of the House Comm. on the Judiciary*, 105th Cong. 42 (1997) (testimony of Sandra A. Sellers, Vice President for Intellectual Property Education and Enforcement, Software Publishers Association), available in 1997 WL 566011 (F.D.C.H.) (urging Congress to “stem the tide of software piracy”).

ryone recognizes that people could copy things in other countries, but, for many rational reasons, our efforts to address this problem should start here and then continue abroad.²⁰ For similar reasons, a rational basis attack on encryption regulations is not successful constitutionally.

Now, allow me to address some of the specific Bill of Rights concerns: the Fourth Amendment, the Fifth Amendment, and the First Amendment.

There is a very interesting disjunction between the debate in the legal world and the debate in the computer world. If you pick up any computer magazine and read about encryption, you will notice that the number one thing that computer professionals and computer users care about, think about, or talk about when they discuss encryption is privacy.²¹ Privacy, privacy, privacy. They say, "I want to use strong encryption because I want my communication and my information to be private." This position seems to me entirely natural. Privacy against unreasonable government searches, of course, is protected in the Constitution's Bill of Rights, primarily by the Fourth Amendment.²² The Fifth Amendment protects other privacy interests.²³

On the other hand, when lawyers attack the encryption regulations, they rely primarily (and sometimes exclusively) on the First Amendment.²⁴ Computer users and computer professionals do not express their desire for strong encryption, generally, in terms of freedom of speech. This disjunction is interesting.

Privacy concerns are raised more squarely than speech issues by the regulation of encryption, so a legal analysis should start with the Fourth Amendment and the Fifth Amendment, which are the constitu-

20. Indeed, in an attempt to deter the willful large-scale copying without a profit motive that can be facilitated by the rise of the Internet, Congress recently amended the copyright law to criminalize that activity. See No Electronic Theft (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997) (codified as amended in scattered sections of 17 U.S.C. and 18 U.S.C.).

21. See, e.g., WHITFIELD DIFFIE & SUSAN LANDAU, *PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION* 137 (1998) (arguing that "[t]he current debate about cryptography is a debate over the right of the people to protect themselves against surveillance").

22. See *Katz v. United States*, 389 U.S. 347, 350 (1967).

23. See *Fisher v. United States*, 425 U.S. 391, 399 (1976) ("[O]ne of the several purposes served by the constitutional privilege against compelled testimonial self-incrimination is that of protecting personal privacy.").

24. See, e.g., *Junger v. Daley*, 8 F. Supp.2d 708, 711-12, 723 (N.D. Ohio 1998); *Bernstein v. United States Dep't of State*, 922 F. Supp. 1426, 1428, 1430-31, 1433-34 (N.D. Cal. 1996), *aff'd*, 176 F.3d 1132 (2-1 decision), *opinion withdrawn pending rehearing en banc*, ___ F.3d ___ (1999), available in No. 97-16686, 1999 WL 782073 (9th Cir. Sept. 30, 1999).

tional bases for privacy.²⁵ However, I do not know how much more we actually need to go into that today because I think Professor Froomkin, though he did not address the issue directly, in the end, would concede that the current export regulations do not violate the Fourth and Fifth Amendments. And, I think he would concede that under some hypothetical regime (without describing or advocating any specific regime), if a law were passed regulating the domestic use of encryption, of the kind that has been under discussion, such a law would not violate the Fourth and Fifth Amendments either.²⁶ Therefore, I shall discuss these issues only briefly.

Basically, under the Fourth Amendment, any plausible regime (even for domestic regulation) would still require, as Special Agent Smith said earlier, a court order or a search warrant.²⁷ Of course, the Fourth Amendment does not say that people have an absolute right of privacy; it says no unreasonable searches or seizures should take place.²⁸ Specifically, it says “[t]he right of people to be secure . . . against unreasonable searches and seizures, shall not be violated.”²⁹ The Fourth Amendment has been used to balance privacy against government intrusions since the Republic was founded. As long as any search of encrypted materials were done in a way that was not unreasonable, it would not violate the Fourth Amendment. Providing for judicial oversight will go a long way towards ensuring the reasonableness that the Fourth Amendment requires.

The Fifth Amendment includes the privilege against self-incrimination.³⁰ This has been interpreted to mean that a person cannot be forced to make statements that are “compelled,” “testimonial,” and “incriminating.”³¹ If a hypothetical regulation were to require that a key be given, upon presentation of appropriate process, to the government by the company that manufactured the software product, this

25. I can understand that more privacy or not having privacy can have an incidental effect on speech, but I still think that privacy is the place to start the analysis.

26. See Froomkin, *supra* note 2, at 30-31.

27. See Charles Barry Smith, *Current U.S. Encryption Regulations: A Federal Law Enforcement Perspective*, 3 LEGIS & PUB. POL’Y 11, 13-14, 19 (1999).

28. See U.S. CONST. amend. IV.

29. *Id.*

30. See U.S. CONST. amend. V (“nor shall [any person] be compelled in any criminal case to be a witness against himself . . .”).

31. See *Fisher v. United States*, 425 U.S. 391, 408-10 (1976) (noting that Fifth Amendment protects accused from being “compelled to make a *testimonial* communication that is incriminating”). See also *Doe v. United States*, 487 U.S. 201, 212 (1988) (stating that policy considerations dictate that Fifth Amendment be used to resist compelled disclosures of incriminating information); *Schmerber v. California*, 384 U.S. 757, 761 (1966) (restricting Fifth Amendment protections to statements of “testimonial” or “communicative” nature).

procedure would not be considered to have “compelled” the software user in violation of their Fifth Amendment right. Even if the key were hypothetically required to be stored with a third party in advance of using the product, such an arguably compelled disclosure would not be “testimonial” under the Supreme Court’s interpretations. Notably, in a case from 1988, *Doe v. United States*, the Court held that an order compelling a person to execute a form consenting to turn over his bank records did not violate the Fifth Amendment because the form was not testimonial.³² The real, non-hypothetical export regulations that are actually the subject of today’s discussion do not have any such required procedures for domestic use and, in fact, do not even reach domestic use.

Thus, the lawyers arguing cases about the current export regulations are left to fall back on the First Amendment, whose protections provide us with the truer point of contention here. Today, Professor Froomkin focused his First Amendment discussion on the issue of whether source code is protected speech.³³ He said that while it may be a close case, he does not personally think it is so close; he believes that source code is protected speech.

Now, even if that were the state of the law, it is important to think about how that conclusion might affect a constitutional analysis. It would not be determinative as to the constitutionality of the export regulations. Rather, it would provide the framework for the analysis. Such a conclusion is not the end of the analysis, but the beginning.

Regardless of whether source code is protected speech, it is instructions to a machine. After all, the point of it is to encrypt data, right? Thus, source code has dual purposes: It could be an interpersonal communication or a technological instruction.

Similarly, a gun could be used for protected speech. I could be at a political protest and wave a gun around; I could wave an Uzi around. Does that mean that it could be used for protected speech, that it has communicative impact? Of course it could. Does that mean it could not be regulated? Of course not. The conclusion that an action can be used for protected speech does not immunize the speech; rather, it provides the constitutional framework within which to analyze the speech.

That constitutional framework is well established. I am sure all of you who have taken a constitutional law course are familiar with

32. See *Doe*, 487 U.S. at 215, 219.

33. See Froomkin, *supra* note 2, at 32-33.

the standards of *United States v. O'Brien*,³⁴ which governs cases where a government regulation of conduct threatens, in particular applications, to impose incidental restrictions on protected expression.

The *O'Brien* case had interesting facts; it involved a person who was prosecuted for burning his draft card at a Vietnam-era anti-war rally on the steps of the South Boston Courthouse.³⁵ You might wonder what could be more protected speech than burning a draft card at a Vietnam-era rally. But, the Supreme Court did not say that burning a draft card at a rally is protected speech, and ergo the law prohibiting destruction of the draft card is automatically unconstitutional. Rather, the Court used the fact that protected speech was implicated as a way to structure its analysis. The Court reasoned that the central question was: *Why* is the government suppressing this activity which implicates protected speech?³⁶ Moreover, the Supreme Court structured the analysis by asking: What is the government's interest in suppressing this speech, in suppressing the activity/speech? Is that governmental interest related to why that speech is protected, and is the regulation substantially overbroad? Does it suppress more speech than is necessary?³⁷

Well, today you heard from the FBI, as well as from the Secret Service, that the reason the government is concerned about encryption is that evidence is increasingly found in electronic form in all kinds of criminal cases. For example, drug dealers do not just use a little black book these days; they use a palm-sized personal organizer. Counterfeiters use personal computers as a means of generating their counterfeit money. And, much of the evidence necessary to investigate and prosecute crimes is going to be found on computers. If evidence is encrypted, law enforcement simply does not have a case. One can try to give law enforcement more resources, but it must be conceded that the biggest computers will not be able to crack the best encryption. Any mathematician would agree with that.³⁸ The government interest is not in suppressing speech, but in protecting the public safety.

34. 391 U.S. 367 (1968).

35. *See id.* at 369.

36. *See id.* at 376-77.

37. Under *O'Brien*, an incidental restriction on expression will be sustained if "it is within the constitutional power of the Government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." *Id.* at 377.

38. *See, e.g.,* ANDRÉ BACARD, *THE COMPUTER PRIVACY HANDBOOK* 77 (1995) ("[N]obody has been able to *publicly* demonstrate how to break [high quality] crypto.").

Now, whether or not the speech is restricted substantially more than it needs to be is hard to measure because, currently, there is no domestic restriction whatsoever. The export regulations, of course, are limited to items of export and, even within the world of export, are limited to narrow categories of products. It is hard to discuss whether a hypothetical domestic regulation would be overbroad, but it seems overzealous to suggest that any domestic regulation would unquestionably be overbroad. Certainly, any hypothetical domestic regulation should put no more incidental restriction on free speech than would be essential. Any law should be written in such a way as not to burden substantially more speech than necessary.³⁹

With two minutes left, let me close by taking a broader view. I have had industry representatives say to me, "Look, David. Cars hurt people, but the United States does not ban cars, do we? So, why are you saying we should ban encryption?" My first response to such criticism is to point out that I am not saying (and nobody who would speak for law enforcement would say) that the United States should ban encryption. Encryption is actually good for law enforcement. Use of encryption is good because it prevents hackers from breaking into computers; it prevents economic espionage and other threats to public safety. In addition, law enforcement needs encryption because we have very sensitive communication. Law enforcement is not in favor of banning encryption. However, law enforcement is in favor of a balanced encryption policy that protects public safety.⁴⁰

My second response is that, while the government does not ban cars, it does regulate cars. And, it has regulated cars since the turn of the century in a million different ways, from inspections to environmental regulations to air bags. The automotive industry argued vigorously against such regulation every step of the way. Some would now say, "Let the FBI deal with encryption; public safety is not our problem." But with cars, the American people said, "No, we want the industry to come out with cars that protect the environment. We want the industry to have cars that have air bags." These public safety con-

39. The means chosen to advance the governmental interest should not "burden substantially more speech than is necessary to further the government's legitimate interests." *Turner Broadcasting Co. v. FCC*, 117 S. Ct. 1174, 1186 (1997).

40. See Letter from Janet Reno, Office of the Attorney General, to Members of Congress (July 18, 1997), available in *Letter from Attorney General Janet Reno and Others to Members of Congress Regarding Law Enforcement's Concerns Related to Encryption*, U.S. DEPARTMENT OF JUSTICE (last modified Jan. 6, 1998) <<http://www.usdoj.gov/criminal/cybercrime/aglet.htm>> (urging a "balanced approach that strongly supports commercial and privacy interests but maintains our ability to investigate and prosecute serious crimes").

cerns are similar to the concerns that law enforcement is bringing to the table. Those laws may not be perfectly followed; it is physically possible to drive a car down a one-way street the wrong way or to drive a car that is not in compliance with the environmental laws. But, generally speaking, I think that the automotive regulations have worked well for public safety.

We have lots of other regulations on cars for public safety concerns. These include drivers' licenses, license plates, and vehicle identification numbers. Indeed, in the Oklahoma City bombing case, the way the FBI caught Tim McVeigh was that the agents found the vehicle identification number and traced it to that van.⁴¹

Similarly, some restrictions on encryption that can provide a means for law enforcement to detect and prosecute criminals should be constitutional. The wisdom of such means should ultimately be decided by the people, as a policy matter. As they have demonstrated with automotive regulation, the American people, through their representatives, are fully competent to balance personal liberty against public safety.

41. *See Picked up for speeding*, THE ECONOMIST, Apr. 29, 1995, at 28.