Encryption, The Internet and Bernstein V. Dep't of Justice: The First Amendment Rescues E-Commerce and Privacy

US export restrictions for encryption software have long denied the Australian IT industry valuable cryptography technology. US attorneys Kurt Wimmer and Dawn Nunziato discuss how freedom of speech and privacy were used to strike down the export restrictions.

It's mid-1999, and the concept of an information economy finally has become more than rhetoric. Internet use has expanded to more than 160 million users worldwide. Electronic commerce is booming, with one company alone reporting more than $1 billion per *month* of sales over the Internet. The need to protect online privacy has seized the attention of consumer advocates and legislators from Washington to Brussels. Concerns over protecting mission-critical computer systems from hackers are at an all-time high following several devastating virus attacks. U.S. software companies are seeking to further their access to an enormous global market.

And the development and export of encryption software – the one technological means to protect the integrity of e-commerce and computer systems and guard personal privacy on the Internet – is under attack by the U.S. government.

What's wrong with this picture?

Encryption – mathematical methods for encoding or scrambling the contents of written or spoken communication so that only the intended recipient can decrypt and access the communication – is widely regarded as the key to secure communications on the Internet. E-commerce relies on strong encryption to protect sensitive credit card and financial data, and Internet users have demanded greater protections for their privacy in both commercial and personal transactions. But the effectiveness of strong encryption to protect privacy has led to concerns by the law enforcement community that international terrorists could use encryption to keep their communications secret from law enforcement. This controversy has led the U.S. federal government to regulate encryption software as a munition – under this view, it can only be exported with a licence from federal authorities. And because information posted on the Internet generally can be accessed from anywhere in the world, the Administration has taken the position that posting source code for encryption software on the Internet is an "export" that cannot occur unless the government grants the author a licence.

This standoff was broken decidedly recently by a combination of the First Amendment, the Ninth Circuit Court of Appeals in San Francisco, and a tenacious young mathematics professor named Daniel Bernstein. In a groundbreaking decision, the Ninth Circuit held that computer source code was expression protected by the First Amendment, and that the government's regulation of encryption source code effected an unconstitutional prior restraint on protected expression. In its 2-1 decision in *Bernstein* v. *U.S. Dep't of Justice*, the court also championed the importance of protecting the privacy of communications and transactions in the electronic realm. Similar constitutional challenges to government regulation of encryption software are currently pending in the D.C. Circuit and the Sixth Circuit, and Supreme Court review of this issue is likely. (Covington & Burling represents a group of *amici* challenging the government regulations in all three circuits, including the Electronic Privacy Information Center, Center for Democracy and Technology, National Association of Manufacturers, Internet Society, American Civil Liberties Union, as well as several world-renowned cryptographers.)

BACKGROUND

This case originated when Daniel Bernstein, then a graduate mathematics student at the University of California at Berkeley, developed a mathematical encryption formula. His formula was expressed in both a scientific paper and in source code, in a high-level computer programming language called "C". Bernstein sought to publish both the source code and the scientific paper through ordinary channels of scientific interchange – including the Internet, the medium of choice for scientists to debate their methods and conclusions – for evaluation, testing, and critique by his peers. In its Export Administration Regulations, the U.S. Department of Commerce requires anyone wishing to "export" (defined to include publication via the Internet) encryption software to receive a government licence. The licence may be withheld if the Bureau of Export Administration concludes that publication is not "consistent with U.S. national security and foreign policy interests." Although an unfavourable licensing determination may be appealed to the Executive, there are no time constraints placed on executive review, and no judicial review of a licensing determination is provided for under the Regulations.

Bernstein applied for a licence to "export" his encryption source code under the predecessor regulatory regime to the Export Administration Regulations. Upon being denied a licence, he filed suit, claiming that the regulations imposed an unconstitutional prior restraint on protected expression.

THE FIRST AMENDMENT'S SCOPE IN THE DIGITAL ERA

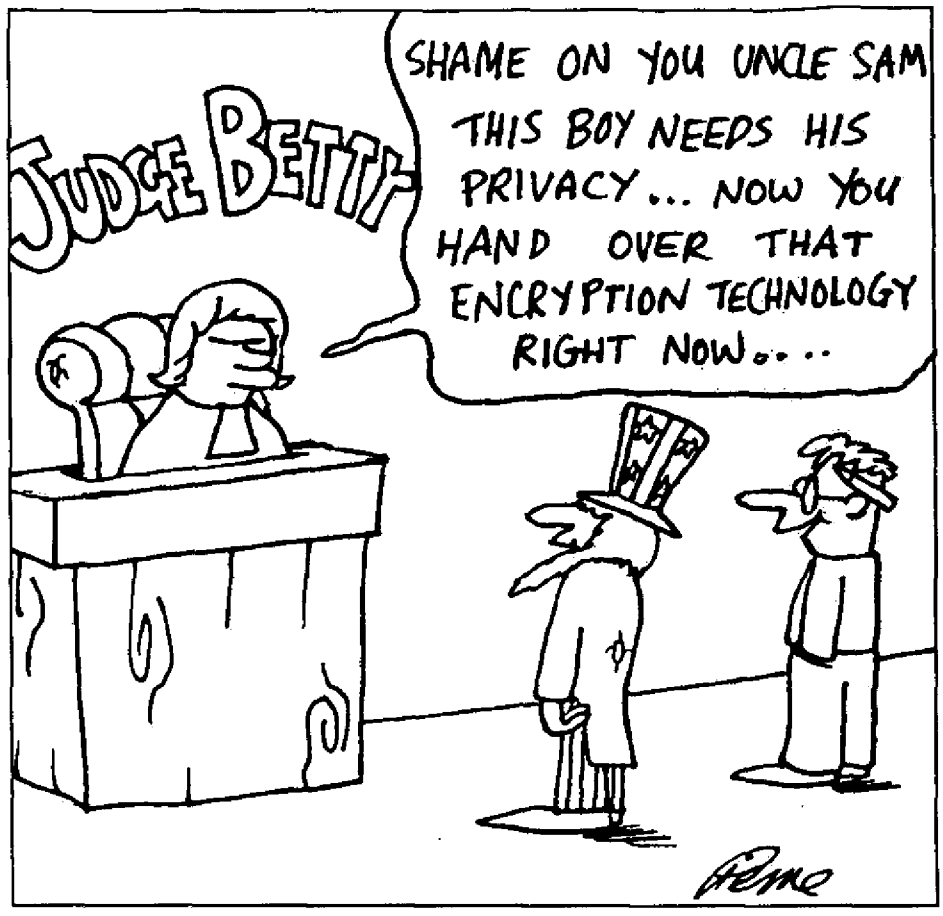
In addressing Bernstein's constitutional challenge, the Ninth Circuit first had to determine whether "computer source code" was expression protected by the First Amendment. This posed a rather novel legal question. It is well established that the spoken and written word are within the ambit of First Amendment protection because of their power to

communicate ideas or emotions to human beings. But does code written in computer programming language really merit First Amendment protection? Does it serve the same sort of communicative role as other forms of protected expression? Even if it has certain communicative elements or features, are these overwhelmed by its functional aspects, as the government argued? In the First Amendment speech/conduct dichotomy, does source code – given its functional qualities – fall on the less-protected "conduct" side of this dichotomy?

Computer source code – which is written in English-like programming languages such as C and BASIC – is distinct from computer object code – which is written in 0s and 1s. While object code directly controls the functioning of a computer, source code can be read and understood by humans and can be used by programmers and mathematicians to communicate with one another. In fact, Bernstein argued that he and his fellow scientists often used source code as a vehicle for communicating mathematical theories on the science of cryptography with precision and mathematical rigour. But, the government contended, even if source code is expressive in some limited sense, it is essentially *functional* expression deserving of limited First Amendment protection. In any case, the government argued, regulation of encryption software is directed toward the functional aspects of such code – its ability (once translated into object code) to encrypt text, and not at all at the expressive aspects of the code or ideas embodied within it.

In her decision, Judge Betty Fletcher held that, despite its functional aspects, computer source code merits full protection under the First Amendment. In declining to afford reduced protection for source code because of its functional features, she explained:

> *[T]he government's argument, distilled to its essence, suggests that even one drop of "direct functionality" overwhelms any constitutional protection that expression might otherwise enjoy. This cannot be so. The distinction urged on us by the government would prove too much in this era of rapidly evolving computer capabilities. The fact that computers will soon be able to respond directly to spoken commands, for example, should not confer on the government the unfettered power to impose prior restraints on speech in an effort to control its "functional" aspects. The First Amendment is concerned with expression, and we reject the notion that the admixture of functionality necessarily puts expression beyond the protections of the Constitution.*



Upon finding source code to be expression protected by the First Amendment, the Court had little difficulty in concluding that the licensing scheme embodied in the Export Administration Regulations imposed an unconstitutional prior restraint. In order to satisfy the dictates of the First Amendment, a pre-publication licensing scheme must either (1) provide for certain procedural safeguards, or (2) fall within an extremely narrow class of cases where the publication at issue would directly and imminently imperil national security (the *Pentagon Papers* standard). In order to be found constitutional, a licensing scheme that fails to meet the *Pentagon Papers* standard must (1) restrain expression for only a specified brief time period; and (2) provide for expeditious judicial review. The government did not contend that the Internet publication of encryption source code would directly and imminently imperil national security, and the court found that the Regulations failed to provide the required procedural safeguards. There are no time limits imposed upon the Executive's review of a denial of a licence, and one denied a licence is not provided with *any* opportunity for judicial review (much less expeditious judicial review). Thus, the Regulations imposed an unconstitutional prior restraint on protected expression in violation of the First Amendment.

PRIVACY IN THE DIGITAL ERA

Beyond its groundbreaking First Amendment holding, the court also recognised that certain Fourth Amendment interests were at stake in the case before it. Judge Fletcher discussed the important role that encryption software plays in preserving the privacy interests of those who communicate and conduct business electronically using technologies such as e-mail, the Internet, and cellular phones. Without well-developed encryption technology, the court explained, we will be unable to carry over to the electronic realm the privacy in our communications and transactions that we have historically enjoyed in the non-electronic realm. In unprecedented language, the court recognised the need

to protect electronic communications and transactions from unwanted surveillance and interception:

> *In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately. Cellular phones are subject to monitoring, email is easily intercepted, and transactions over the Internet are often less than secure. Something as commonplace as furnishing our credit card number, social security number, or bank account number puts each of us at risk. ... Whether we are surveilled by our government, by criminals, or by our neighbours, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty. Viewed from this perspective, the government's efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously, the right against compelled speech, and the right to informational privacy. (Citations omitted).*

In sum, the court recognised that the unfettered development and use of strong encryption technology best serves the public interest in protecting the privacy of electronic communications and transactions.

THE FUTURE OF ENCRYPTION, PRIVACY AND FREE EXPRESSION

The broad holding of *Bernstein* provides a much-needed second step in the establishment of cyber-rights that was begun in *Reno v. ACLU*. In the *Reno* case, the U.S. Supreme Court established that the First Amendment applied in full force in cyberspace. The value of that case lies not only in its holding striking down portions of the Communications Decency Act, but in the scope of its language and analysis. Similarly, the *Bernstein* court now has established that computer source code is protected by the First Amendment and has done so in a decision that recognises that privacy rights are of crucial importance in an age defined by electronic commerce and Internet communication.

The *Bernstein* case thus provides a basis for moving forward. The most immediate benefit is that cryptographers such as Professor Bernstein finally will be able to discuss their science on the Internet effectively and with the protection of the First Amendment. The more global benefits, however, may inure to much broader groups. U.S. software companies that have been hampered in their efforts to market encryption software abroad will be able to more effectively compete with their international counterparts. U.S. companies that wish to secure their communications by exporting encryption software to their partners and employees abroad will be free to do so. Secure electronic commerce will be able to extend past our borders, and U.S. companies will be able to market goods and services effectively to security-conscious consumers around the world. Perhaps most importantly, the e-mail and other Internet communications of individuals everywhere will have the potential to be private.

The path toward the effective use of encryption is not, of course, an entirely clear one. The Department of Justice is considering further attacks to the holding of the panel in *Bernstein*, and it almost certainly either will seek rehearing by the entire court or review by the U.S. Supreme Court. Two other federal Courts of Appeal have cases pending before them involving similar First Amendment challenges to export restrictions on encryption. In *Junger v. Daley*, 8 F. Supp. 2d. 708 (N.D. Ohio 1998), currently pending before the Sixth Circuit, computer law professor Peter Junger was refused a government licence to publish encryption source code via the Internet. Junger is appealing from the district court's decision that source code – because of its functional characteristics – cannot be characterised as "pure speech" and does not merit full protection under the First Amendment. In *Karn v. U.S. Dep't of State*, 925 F. Supp. 1 (D.D.C. 1996), now on remand from the D.C. Circuit, cryptographer Philip Karn was also refused a government licence to publish encryption source code in electronic form. The district court in *Karn* held that, because the government regulations were not motivated by a desire to suppress expression but rather by legitimate national security interests, the First Amendment was not offended. If, as is likely, either the Sixth Circuit or D.C. Circuit companion cases are resolved differently from *Bernstein*, Supreme Court review of this important legal issue is likely.

Kurt Wimmer is a partner in the Washington, D.C. office of Covington & Burling and is chair of its Information Technology practice group. He and David Addis of Covington & Burling are counsel to the amicus group in the Junger case.

Dawn Nunziato is an Associate Professor at George Washington University Law School, where she teaches Internet law, computer law, and intellectual property. While associated with Covington & Burling, she represented the lead amicus group in the Bernstein and Karn cases.