

tial protection for authors. One of Eldred's pro bono lawyers, Larry Lessig of Harvard University, has observed that this new law reneges on the copyright "bargain," which implies that owners have rights over their creative works for a limited time. According to Lessig, "It's important for the court to say 'limited' means 'limited.'" Congress seems to have moved beyond the notion of a reasonable copyright term for no rational reason other than to heap greater rewards on an author's heirs and on corporations. This extension certainly has nothing to do with increasing incentives for authors who will not directly benefit from it.

In my estimation, Boyle's analysis of the romantic author justification for property protection is astute and accurate. Beyond any doubt, this is one factor that has led to the U.S.'s generous copyright protection scheme. I would not, however, underestimate (as he does) the influential role of Locke's labor theory in all of this. Locke's property theory is at the heart of capitalist thinking about property and the necessary link between property-based rewards and incentives. Thus, our intellectual property laws are also grounded in an impulse to reward the author's labor as well as originality.

As recent events illustrate, Boyle does not exaggerate when he warns us about the potential excesses that can accompany this romanticized author vision. And he is obviously right to stress that fair use provisions and the public domain must be adequately preserved in order to provide the raw material for new creative initiatives. As Nietzsche reminds us in *Also Sprach Zarathustra*, all creation (*schaffen*) is really a renewal or recreation (*umschaffen*) of what others have done in the past. Creators find their inspiration in the past. They are constantly retrieving past works or cultural accomplishments and projecting a new light upon them. If we go too far in protecting our intellectual property we run the risk of erecting a formidable fortress around our past traditions that will eventually deplete the common pool of knowledge and wisdom, which are the building blocks for the creators of tomorrow.

The book is less successful when it tries to suggest remedies and alternatives for our flawed copyright laws rooted in the romantic vision of authorship. For instance, Boyle maintains that a new system of software protection is needed but provides precious few details of what this would look like. He argues for expansion of the public domain and more restrictions on the private domain, but once again provides no detailed plan for how this might be accomplished. One recommendation is that copyright should last for twenty years and fair use provisions should be more broadly defined. But this normative recommendation

needs more elaboration, a more precise delineation of which activities fair use will allow. Some of Boyle's proposals are not without merit but they are far too sketchy and unnuanced to be taken seriously by public policy makers.

These are minor problems, however, that only slightly detract from this impressive work. On balance, and keeping in mind the limited focus on the Anglo-American tradition, Professor Boyle has articulated an incisive view of intellectual property that deserves our respect and attention.

*Carroll School of Management, Richard A. Spinello
Boston College, Fulton Hall,
Chestnut Hill, MA 02467, USA*

Privacy on the Line: The Politics of Wiretapping and Encryption by Whitfield Diffie and Susan Landau (Cambridge, MA: The MIT Press, 1998).

The decline of personal privacy in Western democratic societies is usually attributed to the massive computerization of daily activities. It is computers that have made it possible to capture, store, search, link, and access personal data, to an extent simply unimaginable a mere half century ago. Legislation has, in general, not been able to reverse the trend: the need for individuals to maintain some sphere of privacy seems continually pitted against both the needs of the State for security and the needs of private organizations for bureaucratic rationalization.¹ Computer technology, it would appear, is more amenable to fulfilling the latter goals than the former.

This apparent collusion of technology and technocracy need not necessarily be the case: from the scientific arena, one unlikely voice has emerged, seeking to challenge the assumption that computer technology must inevitably work against individual needs for privacy. A small group of pony-tailed mathematicians, with a taste for puzzles, spy stories, and libertarian politics, have proposed that, thanks to new mathematical twists on the ancient art of *cryptology*,²

¹ A good recent overview of privacy legislation is Priscilla Regan's *Legislating Privacy* (Chapel Hill: University of North Carolina Press, 1995).

² A note on terminology: *cryptography* is the science of designing cryptosystems, while *cryptanalysis* is that of breaking them; *cryptology* encompasses both. Designing cryptosystems used to be synonymous with designing *encryption* systems – i.e. technologies providing confidentiality to parties wishing to communicate at a distance; in the last thirty years, however, the scope of cryptology has broadened beyond encryption, to

we can reap the benefits of computerization while still protecting our privacy. While the historical relation of cryptology to national security interests has made the diffusion of these technologies problematic, the explosive popularity of the Internet and the push for electronic commerce has brought much media attention to cryptologists and their craft. Far from shielding their work from social debates, they have actively argued for a vision of computers in society where cryptology plays a positive role.

Their arguments have clustered around two principal themes: firstly, private and public organizations are collecting and linking all types of transactional information, achieving in effect a *dossier society*; yet, new mathematical techniques can provide the means to protect the sphere of transactional privacy, while simultaneously respecting the needs of organizations for fraud detection and rationalization. Secondly, intelligence and law enforcement agencies are quietly ensuring through legislation that the emerging electronic communication infrastructure is wiretap- and surveillance-friendly; again, modern mathematical techniques of encryption offer the means to provide electronic privacy to the masses.

The former argument has been especially well researched and argued by David Chaum, an American cryptologist and entrepreneur, in several widely circulated papers published in the '80s.³ The latter argument is the subject of *Privacy on the Line*, written by Whitfield Diffie and Susan Landau. Diffie, a distinguished engineer at Sun Microsystems, became a seminal figure of modern cryptology in 1976, when he invented, together with Martin Hellman, public-key cryptography.⁴ Landau, a professor of computer science at the University of Massachusetts in Amherst, has chronicled some of the earlier encounters of academic cryptology with the world of military intelligence.⁵ As active participants in the cryptography policy debate, both enjoy access to a wealth of technical and privileged information – an important asset in the secrecy-laden worlds of intelligence and national

include the design of digital signatures, e-cash, voting systems, etc.

³ "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM* **24** (1981): 84–88; "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," *Communications of the ACM* **28** (1985): 1030–1044; "Achieving Electronic Privacy," *Scientific American* (August 1992): 96–101.

⁴ "New Directions in Cryptography," *IEEE Transactions in Information Theory* **22** (1976): 74–84.

⁵ "Primes, Codes, and the National Security Agency," *Notices of the American Mathematical Society* **30**(1): 7–10; "Zero Knowledge and the Department of Defense," *Notices of the American Mathematical Society* **35**(1): 5–12.

security. The stated goal of the book is to use that information to bring some light to rather esoteric technical debates about the fate of cryptography; debates characterized by confusion and misinformation, but which, nonetheless, hold great import to the continuation of the democratic political process. The book is primarily concerned with the construction of these debates within the American political arena, although it does hint at their broader international implications.

Debates about the diffusion of cryptographic technologies firmly entered the public sphere in 1993, when the White House announced its intention to promulgate a new encryption standard. The standard was intended as a response to growing fears by both law enforcement and the intelligence community that the digitalization of communication equipments and widespread availability of high-quality encryption technologies would soon make their work impossible. This new standard, the Escrowed Encryption Standard (EES), consisted of tamper-resistant chips (Clipper), implementing a secret encryption algorithm (Skipjack), to be ultimately embedded into all digital communication equipment sold and used in the United States – fax, modems, phones, etc. As expected, the Clipper chip would perform strong encryption between communicating devices – with the added twist that the keys needed to decode any given exchange would be *escrowed*, that is, stored and available to the proper authorities, given a warrant. The government's original strategy was to promote the adoption of the proposal through a (voluntary) standardization process. This approach met with staunch opposition from business, civil liberties organizations, and cryptologists, and was eventually abandoned, in that specific incarnation at least. Diffie and Landau explain that the government has now turned to export control laws to achieve its aims: under the United States' *International Traffic and Arms Regulations*, cryptographic algorithms are classified as munitions and their diffusion severely restricted, making it much more difficult for American products to compete in the emerging and promising global markets for cryptographic technologies. Recently however, cryptography businesses have been offered looser exporting licenses, *if* they agree to adopt key escrowing technology in the future.

The debate over the shape and availability of cryptographic technologies is thus very much alive, if under new management. Why should we care? As Diffie and Landau succinctly put it, "[i]ntentions can change far more quickly than capabilities" (p. 230). That is, building privacy *into* the technological infrastructure itself is a longer lasting guarantee for political freedom than legislation can ever be. On the reverse side, building *surveillance* into the communications infrastructure, as the EES seeks to do, also

offers a longer lasting guarantee that the expression of dissenting political views will remain a dangerous occupation in the years to come. The book suffers no shortage of examples demonstrating how American citizens have already suffered from political oppression, most notably under Edgar Hoover's reign as chief of the FBI – lasting 48 years and through eight presidencies – or, more recently, during the Watergate affair. Diffie and Landau thus see the stakes of the cryptography policy debate as being no less than the protection of the democratic process itself.

The first level of Diffie and Landau's argument thus firmly locates the cryptographic debate in the political realm. But attempts to prevent citizens from communicating privately are not only antidemocratic, they are useless: the cryptographic genie is already out of the bottle, and its spread is uncontrollable, as cryptologists have made a point of demonstrating over and over. From the distribution of PGP over the Internet, to the recent invention of algorithms that provide confidentiality without using anything resembling the legal definition of encryption,⁶ the technology is out there, Diffie and Landau warn us, and attempts to control it are laughable, incoherent, and ineffective.

As far as law enforcement is concerned, fears of cryptography are also unwarranted, the authors contend. It may well be true that access to encryption will make some wiretaps ineffective. But this is not really a problem since, contrary to common wisdom, wiretaps are not a significant part of police investigation. In fact, in most cases, they could altogether be done away with without major losses to crime-solving capabilities. Using the *Wiretap Report*, a publication of the Administrative Office of the Federal Courts providing statistical information on wiretaps ordered in the previous year, the authors conclude that the value of wiretaps is, at best, wildly exaggerated, and in no way justifies that the entire communication infrastructure of the United States be made surveillance-friendly. Not only is the effectiveness of wiretaps dubious, but the FBI's claim that it will lose law enforcement capabilities because of advances in digital communications simply hasn't been convincingly made: "...police have experienced an unprecedented expansion of their powers of surveillance in almost every area [databases, video cameras, bugs, etc.]. Many of these facilities play far greater roles in criminal investigations than wiretaps, and any loss of investigative power that results from changes in communications technology seems minuscule in comparison" (p. 230). That is, Diffie and Landau

argue, the overall balance of technological advantage has shifted in the favor of law enforcement, not the opposite.

The losses to the intelligence community implied by the diffusion of cryptological technologies remain to be addressed. Here, the problem is compounded: before intelligence organizations can even begin listening in, they must select interesting sources among the multitude of possible data sources. Cryptography threatens to make this process of *traffic selection* next to impossible, as monitoring devices will be incapable of determining the intelligence value of an encrypted data source in the first place. Then, of course, if the source is determined to be of interest, intelligence agencies must still decode it in order to use it. While Diffie and Landau recognize these problems, they contend that they should be viewed as one small factor within many other changes in the intelligence gathering landscape. While cryptography may render a portion of the communication bandwidth unintelligible, new opportunities will abound: "[o]n the other hand, improvements in communications and increasing human dependence on communications will open new areas of intelligence. Network penetration will make it possible to capture information that is being stored rather than communicated, and such information is less likely to be encrypted" (p. 235). Cheaper cellular telephony will open entire segments of the telecommunications markets to the prying eyes of intelligence organizations. Overall, the future of communications intelligence seems brighter than ever, with or without the availability of cryptography.

As their final (and most surprising) call for deregulating cryptography, Diffie and Landau argue that "[it] is much less successful at concealing patterns of communication than at concealing the contents of messages" (p. 235).⁷ That is, while cryptography may hamper some prying into individual's private conversations, it is mostly useless in the sphere of transactional data, the vast data banks of information we contribute to with every phone call, credit-card purchase, plane reservation. Diffie and Landau's surprise argument is thus that intelligence and law enforcement agencies need not fear cryptography, for increasing reliance on computer networks will, ultimately, *increase* the amount of data available to them for electronic surveillance. To summarize, the authors claim that we should value cryptography because it can uniquely protect the privacy of our communications. Yet, we needn't

⁶ See Ronald Rivest, "Chaffing and Winnowing: Confidentiality without Encryption," *CryptoBytes* 4(1). Available at <theory.lcs.mit.edu/~rivest/>.

⁷ This is debatable. David Chaum's inquiries into anonymous electronic transactions launched a research industry that flourishes to this day. See for example, Michael K. Reiter and Aviel D. Rubin, "Anonymous Web Transactions with Crowds," *Communications of the ACM* 42(2): 32–38.

fear cryptography, because privacy can be breached in many other ways!

This ambivalence underlines the major shortcoming of the book. On the one hand, it provides a highly useful and up-to-date map of the intricate law enforcement and security policies which determine the extent to which American citizens may be subjected to direct surveillance. On the other hand, it almost entirely ignores a host of other factors which play a significant role in shaping the forms of privacy and democracy in a computerized society: cultural

norms, business interests, and citizen involvement, for example. For Diffie and Landau, the single locus of power seems to lie with the free circulation of encryption: let technology be, and all else will follow. One might answer: cryptography alone does not privacy make; and privacy alone does not democracy make.

Dept. of Science and Technology Studies,
Rensselaer Polytechnic Institute,
Troy, New York, USA. Jean-François Blanchette