to put PGP on the Internet for use in the U.S., and in conformance with export controls.

By the end of the decade, the progress of electronic commerce had overtaken the key escrow debate, and the government had ended its criminal investigation without an indictment. Zimmermann built a business around PGP (see `www.pgp.com`), while still allowing free downloads for individuals. His web site contains testimonials from human rights groups in Eastern Europe and Guatemala attesting to the liberating force of secret communication among individuals and agencies working against oppressive regimes. Zimmermann had won.

Sort of.

ENCRYPTION REGULATION ABROAD

Some countries have adjusted to multiple uses of the same encryption algorithms, for commercial, military, and conspiratorial purposes. For example, the Chinese government strictly regulates the sale of encryption products, "to protect information safety, to safeguard the legal interests of citizens and organizations, and to ensure the safety and interests of the nation." In 2007, the United Kingdom enacted laws requiring the disclosure of encryption keys to government authorities investigating criminal or terror investigations, on penalty of up to five years in prison.

Cryptography Unsettled

Today, every banking and credit card transaction over the Web is encrypted. There is widespread concern about information security, identity theft, and degradation of personal privacy. PGP and other high-quality email encryption programs are widely available—many for free.

But very little email is encrypted today. Human rights groups use encrypted email. People with something to hide probably encrypt their email. But most of us don't bother encrypting our email. In fact, millions of people use Gmail, willingly trading their privacy for the benefits of free, reliable service. Google's computers scan every email, and supply advertisements related to the subject matter. Google might turn over email to the government in response to a court order, without challenging the demand. Why are we so unconcerned about email privacy?

Why are we so unconcerned about email privacy?

First, there is still little awareness of how easily our email can be captured as the packets flow through the Internet. The password requests needed to get our email out of the mail server may provide the

Spying on Citizens

Historically, spying on citizens required a warrant (since citizens have an expectation of privacy), but spying on foreigners did not. A series of executive orders and laws intended to combat terrorism allow the government to inspect bits that are on their way into or out of the country. (Perhaps even a phone call to an airline, if it is answered by a call center in India.) Also excluded from judicial oversight is any "surveillance directed at a person reasonably believed to be located outside of the United States," whether that person is a U.S. citizen or not. Such developments may stimulate encryption of electronic communications, and hence in the end prove to be counterproductive. That in turn might renew efforts to criminalize encryption of email and telephone communications in the U.S.

illusion of security, but they do nothing to protect the messages themselves from being sniffed as they float through fibers, wires, and the air. The world's biggest eavesdropping enterprise is very poorly known. It is the international ECHELON system, which automatically monitors data communications to and from satellites that relay Internet traffic. ECHELON is a cooperative project of the U.S. and several of its allies, and is the descendant of communications intelligence systems from the time of the Second World War. But it is up-to-date technologically. If your email messages use words that turn up in ECHELON's dictionary, they may get a close look.

Second, there is little concern because most ordinary citizens feel they have little to hide, so why would anyone bother looking? They are not considering the vastly increased capacity for automatic monitoring that governments now possess—the driftnet monitoring of which Zimmermann warned.

Finally, encrypted email is not built into the Internet infrastructure in the way encrypted web browsing is. You have to use nonstandard software, and the people you communicate with have to use some compatible software. In commercial settings, companies may not want to make encryption easy for office workers. They have an interest—and in many cases, regulatory requirements—to watch out for criminal activities. And they may not want to suggest that email is being kept private if they are unable to make that guarantee, out of fear of liability if unsecured email falls into the wrong hands.

It is not just email and credit card numbers that might be encrypted. Instant Messaging and VoIP telephone conversations are just packets flowing through the Internet that can be encrypted like anything else. Some Internet phone software (such as Skype) encrypts conversations, and there are several other products under development—including one led by Zimmermann him-

self—to create easy-to-use encryption software for Internet telephone conversations. But for the most part, digital communications are open, and Eve the evil eavesdropper, or anyone else, can listen in.

Overall, the public seems unconcerned about privacy of communication today, and the privacy fervor that permeated the crypto wars a decade ago is nowhere to be seen. In a very real sense, the dystopian predictions of both sides of that debate are being realized: On the one hand, encryption technology is readily available around the world, and people can hide the contents of their messages, just as law enforcement feared—there is widespread speculation about Al Qaeda's use of PGP, for example. At the same time, the spread of the Internet has been accompanied by an increase in surveillance, just as the opponents of encryption regulation feared.

So although outright prohibitions on encryption are now impossible, the social and systems aspects of encryption remain in an unstable equilibrium. Will some information privacy catastrophe spark a massive re-education of the Internet-using public, or massive regulatory changes to corporate practice? Will some major supplier of email services and software, responding to consumers wary of information theft and government surveillance, make encrypted email the default option?

The bottom-line question is this: As encryption becomes as ordinary a tool for personal messages as it already is for commercial transactions, will the benefits to personal privacy, free expression, and human liberty outweigh the costs to law enforcement and national intelligence, whose capacity to eavesdrop and wiretap will be at an end?

Whatever the future of encrypted communication, encryption technology has another use. Perfect copies and instant communication have blown the legal notion of "intellectual property" into billions of bits of teenage movie and music downloads. Encryption is the tool used to lock movies so only certain people can see them and to lock songs so only certain people can hear them—to put a hard shell around this part of the digital explosion. The changed meaning of copyright is the next stop on our tour of the exploded landscape.