Free Speech Online and Offline

Ross Anderson
Cambridge University

The lack of an understanding of the relationship between cause and effect makes most governments incompetent at balancing public policy goals that affect cyberspace.

Esther Dyson famously argued that as the world will never be perfect, whether online or offline, it is foolish to expect higher standards on the Internet than we accept in "real life." Legislators are now turning this argument around, arguing that they must restrict traditional offline freedoms in order to regulate cyberspace.

A shocking example is an export control bill currently before Britain's Parliament (http://www.cl.cam.ac.uk/~rja14/exportbill.html). This bill will enable Tony Blair's government to impose licensing restrictions on collaborations between scientists in the UK and elsewhere, to take powers to review and suppress scientific papers prior to publication, and even to license foreign students taught by British university teachers.

INTANGIBLE EXPORTS

The justification offered for this is a European agreement to control the "intangible export" of technology (http://projects.sipri.se/expcon/eudu/eureg_0006.htm).

During the late 1990s, arms export regulations prevented US nationals from making cryptographic software available on their Web pages or sending it abroad by e-mail. Phil Zimmermann, the author of the popular PGP encryption program, was investigated by a Grand Jury for letting the program "escape" to the Internet. The law was ridiculed by students wearing T-shirts printed with encryption source code (Warning—This T-shirt is a munition!) and challenged in the courts as an affront to free speech. Meanwhile, European engineers made crypto software freely available.

The Clinton administration fought back, with Al Gore pushing European governments to fall in line. After Tony Blair was elected in 1997, the British government became eager to help, but Parliament was unimpressed by their first attempt in 1998 to impose export controls on intangibles. The government then tried an end run around Parliament by quietly negotiating a Europe-wide agreement that they now say we have no choice about implementing.

Individual European countries have a lot of latitude about how they implement this agreement, but the British approach is draconian. The proposed law will give ministers wide powers to regulate the transfer of technologies that could have harmful effects. Ministers admitted in Parliament that their overriding concern was to leave no loopholes—no T-shirts, no bar codes, no faxes, no covert channels—through which controlled information could lawfully leave the country. This law even allows the government to control "nondocumentary transfers" (read: speaking to foreigners) in cases in which the technology could be used for certain types of weapons, such as guided missiles.

0018-9162/02/$17.00 © 2002 IEEE

As I am currently on sabbatical at MIT, helping US students think about integrating inertial navigation with sensor networks, it's lucky the bill isn't law yet. This new research topic only came up recently in a seminar, and I was able to pitch in some ideas at once. If I needed an arms export license to take part in the discussion, getting it would have taken weeks or even months, and the value of spontaneous interaction would have been lost.

Controlling physical exports is easy, at least in principle. But once you try to control the electronic export of software, designs, specifications, and technical support, it is hard not to end up controlling speech as well—the dividing line is too blurred. So is the concept of "abroad."

It is quite common for an e-mail message between two British scientists to travel via the US, and an e-mail message sent to me at Cambridge, England, will be forwarded to Cambridge, Massachusetts, if that's where my body happens to be.

If we give officials enough regulatory discretion to deal with all this, they have the power to interfere with speech, too—and much else. For example, the UK bill extends the scope of arms export controls from a few hundred "obvious" armament vendors to thousands of innocuous software companies.

What about the millions of people who use online services in foreign countries? Will it become an offense for a Brit who works with high technology to have an e-mail account at a US provider, like AOL, to which messages get forwarded when she's traveling?

REGULATORY OVERSPILL

While the struggle to amend this particular bill is primarily a matter for Britain's scientific and engineering establishment, it is an example of a wider and worrying trend—of toxic overspill from attempts to regulate the Internet.

There are many more examples. In the US, Hollywood's anxiety about digital copying led to the Digital Millennium Copyright Act. This legislation gives special status to mechanisms that enforce copyright claims: Circumventing them is now an offense. So manufacturers are now bundling copyright protection with other, more objectionable, mechanisms, such as accessory control. For example, one game console manufacturer builds into its memory cartridges a chip that performs some copyright control functions, but their main purpose appears to be preventing other manufacturers from producing compatible devices. There is no obvious way to reconcile the tension between public policies on copyright and on competition.

The antiterrorism laws that many nations now have provide more examples of regulatory overspill and overkill. In Britain, for example, terrorism is defined (http://www.legislation.hmso.gov.uk/acts/acts2000/20000011.htm) as acting in concert with others, for political or religious purposes, using certain means (including violence, property damage, or interfering with a computer system) that achieve certain ends (including death, property damage, or risks to public health). This definition followed police scaremongering about cyberterrorism, and it has a curious effect. Should I, here on US soil, voice support for the Icelandic Medical Association's boycott (http://www.mannvernd.is/ english/index.html) of that country's controversial genetic database—which, according to the government in Reykjavik, is degrading the information flows they need to manage public health—I would become an international terrorist on the spot. (Perhaps I'd better say no more.)

The struggle to amend this bill is an example of toxic overspill from attempts to regulate the Internet.

Meanwhile, worries about cybercrime are leading to a Europe-wide arrest warrant that overturns the time-honored principle of dual criminality—that you can only be extradited from one country to another if there is prima facie evidence that you've done something that's a crime according to the laws of both countries. Now Germany has strict hate speech laws—*Mein Kampf* is a banned book—while Britain does not. Right now, I could put an excerpt from that book on my Web site in the UK (or the US) but not in Germany. However, the new arrest warrant would allow the German police to extradite me from Britain for an offense that doesn't exist in British or American law. Thus, free speech rights online may be reduced to the lowest common denominator among the signatory nations.

At a conference in Berlin in 2000, the German federal justice minister said that her proudest achievement in office had been to stop Amazon.com from selling *Mein Kampf* in Germany, and that her top ambition was to stop the company from selling it in Arizona, too.

European arrest warrants do not quite go that far. But in the near future, if Amazon sold a copy of this book to a history professor in Finland, and Amazon's Jeff Bezos were later passing through Madrid, the Germans could have him hauled off to Berlin for trial.

WHY ARE THERE SO MANY BAD LAWS?

Why do we get so many bad laws about information? Several factors are at work.

Much of the cyberlaw that has been rushed through in the past few years will need substantial revision.

First, the Internet is no different from any other new frontier in that businessmen compete to make money out of it, while bureaucrats compete to build empires regulating it. The dot-com bubble is being followed by a dot-gov version. However, while poorly thought-out business plans run out of cash and disappear, poorly thought-out laws remain, together with irrelevant services and bureaucratic overhead.

Second, the Internet is different from, for example, the Wild West in that the often harsh law enforcement of those times could be replaced and updated as new states were formed. There is no such natural opportunity to revise cyberlaw.

Third, the laws in newly created states were written by people elected by the folks who lived there. This isn't true at all for cyberspace, which is regulated by the same politicians and senior officials who run meatspace—and are beholden to its vested interests.

Fourth, there are issues of understanding as well as motivation. Cyberspace is more different from Arizona than Arizona is from New York. As politics is about managing the tradeoffs between competing legitimate rights and interests, good public policy requires a good understanding of the relationship between cause and effect. The lack of this understanding makes most governments incompetent at balancing public policy goals that affect cyberspace. It's hard enough to exchange e-mail with a government department, let alone teaching it how to draft laws that catch only the phenomena they are intended to catch.

Fifth, many of the bad laws have to do—in some broad sense—with computer security, or at least with the Internet's perceived vulnerability to hackers, bomb makers, credit card thieves, pornographers, and other undesirables.

There is a huge amount of hype from the computer security industry—when people get fed up with hearing about hackers, the story becomes one of "cyberterrorism." There are few or no balancing voices, as the interests of almost everyone involved in the security industry—vendors, government agencies, regulators, researchers—lie in talking up the threats. Journalists like the scare stories more than the rebuttals. As with Y2K, the still small voice of reason goes unheard.

WHAT IS TO BE DONE?

In the shorter term, there is much that individual engineers can do. Engineers and lawyers have at last started to talk to each other about technology policy, while colleagues and I are currently promoting cross-disciplinary research at the boundary between information security and economics.

In the longer term, much of the cyberlaw that has been rushed through in the past few years will need substantial revision. In the US, that might happen through the Supreme Court, though it might be unwise to rely on that completely. In the European Union, engineers should be seeking to influence the constitutional negotiations getting under way for the community's enlargement in 2005. We could try to introduce a mechanism that automatically sends technology policy directives for revision every five to 10 years.

Whatever the mechanisms, we technologists need more influence over the development of technology law. Our profession has grown rapidly in numbers over the past quarter century, and our contribution to economic development is decisive. However, our political clout hasn't grown to match our numbers. We have been too busy making the world a better, richer place to spend time infiltrating the citadels of power. Fixing this political deficit is now not just in our own best interest, but in everybody's. ■

***Ross Anderson**, who wrote this article while on sabbatical at MIT, leads the security group at the Computer Laboratory, Cambridge University. He is the author of* Security Engineering: A Guide to Building Dependable Distributed Systems *(John Wiley & Sons, New York, 2001). Contact him at ross.anderson@cl.cam.ac.uk.*