Society | DOI:10.1145/2063176.2063184 Samuel Greengard

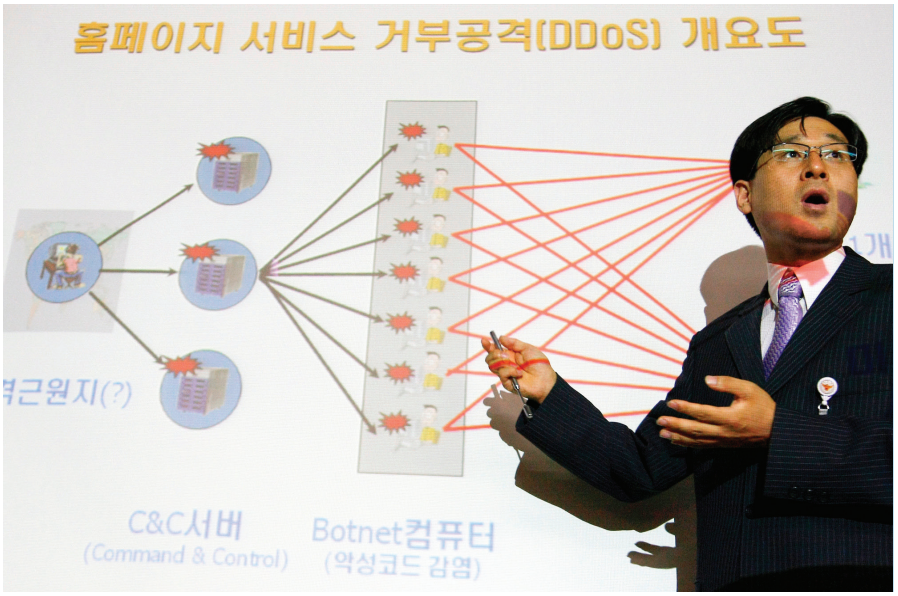
Law and Disorder

International law has always been a murky and Byzantine area. However, the Internet and digital technology have raised the stakes, the risks, and the challenges.

Getting people and countries to agree on things has never been the simplest of matters. However, in the age of the Internet and digital technology, there is no question that the stakes are greater than ever. "The ability to build a legal framework across nations is an increasingly difficult task," states Michael Geist, research chair in Internet and e-commerce law at the University of Ottawa.

Cyberlaw—essentially real-world law extended to the virtual world—is at the center of an increasingly contentious battle over rights, responsibilities, and resources. Unfortunately, there is no international court and no global legislature. Antagonists may be individuals, cybergangs, or nation-states. And new forms of crime—resulting from the rise in Internet commerce, as well as digital goods—has created nettlesome challenges that touch diverse areas: theft, defamation, copyright infringement, intellectual property theft, child pornography, espionage and terrorism, to name a few.

"The legal system is struggling to keep up with today's technology," states Jonathan Bick, an adjunct professor of Internet law at Rutgers University Law School. Unfortunately, these days, there are more questions than answers. How is technology changing the way countries approach matters as diverse as international crime and content ownership? How is it altering business? And what are governments doing to bring order to cyberspace?



AP PHOTO/YONHAP, HWANG KWANG-MO

An official gives a press briefing about cyberattacks at the National Police Agency in Seoul, South Korea on July 8, 2009. South Korean intelligence officials believe North Korea or pro-Pyongyang forces in South Korea are responsible for the disruptive cyberattacks.

Legal Griefs

Since the emergence of the public Internet in the mid-1990s, people and communications have become intertwined in ways that would have once been unimaginable. Nearly 2.1 billion people—about 30% of the world's population—now use the Internet. Globally connected commerce, supply chains, and workplaces have become the norm. In fact, about U.S. $10 trillion in global online transactions currently take place and the figure could rise to U.S. $24 trillion by 2020, according to the Council of Europe (CoE). By contrast, the current gross world product is about $63 trillion, according to the World Bank.

Of course, where there is money there are thieves and scofflaws. Yet keeping up with a fast-changing digital environment has proven overwhelming. One of the biggest challenges is the simple fact that "what's illegal in one country may not be illegal in another," says Pauline C. Reich, director of the Asia-Pacific Cyberlaw, Cybercrime and Internet Security Institute and co-author of *Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization*.

But the issues and challenges don't stop there. "Individual countries can pass whatever laws they like. If you can't arrest people and enforce the law it's not very useful," Bick notes. The root problem is that there is no such thing as international law. "It's nothing more than a series of bilateral treaties, conventions, and governments claiming jurisdiction over certain laws," says Bick. "It's up to individual countries to decide whether they want to comply with another country's laws."

Many crimes, such as identify theft and child pornography, already have clearly established laws and police protocols that span international borders. The prickliest issues revolve around areas such as print, broadcast, and telecommunications, where industrial-age business models and digital-age sharing and stealing redefine usage boundaries. The challenge, says Jan Kleissen, director of standards for CoE, is balancing risk with rights. "The Internet is critical for the exercise of people's rights and freedoms, as well as for their everyday activities," he explains.

There is certainly no shortage of legal disputes. For example, the United

Arab Emirates, citing security concerns, suspended data access and text messaging for 500,000 BlackBerry devices in 2010 before it struck a deal with Research In Motion (RIM) that may have placed a server inside the country, with the government able to access it. A similar clash took place in India in 2008. Security agencies there threatened to shut down BlackBerry service unless RIM allowed the government to intercept messages. The company refused, and after a series of discussions, the Indian government relented.

Bick argues that a great deal of the legal jostling taking place in the international arena revolves around economics rather than overarching legal reasons. "In some cases, governments and companies use their own courts, which they control, to promote a competitive advantage." That is nothing new, Geist says. "More powerful countries, such as the U.S, often attempt to tilt international standards in their favor."

Yet it is not only information and money that are in the legal crosshairs. This past June, Japan's parliament enacted legislation criminalizing the creation or distribution of computer viruses. The goal of cracking down on cybercrime seems noble enough, but critics stated that the new law could infringe on constitutionally guaranteed personal liberties. The Japanese Parliament later revised the law to allow legitimate uses. Of course, Japan does not exist in a vacuum. Barring an international treaty, the law is unlikely to cut down on malware in any significant way; malware writers can always find a safe haven.

"Individual countries can pass whatever laws they like," notes Jonathan Bick. "If you can't arrest people and enforce the law, it's not very useful."

The issues grow even more complex when hackers breach systems in other countries and cybercriminals plant botnets on computers. In July 2009, South Korea accused North Korea of launching cyberattacks against government, news media, and financial Web sites—and spreading botnets. The U.S. was also the target of these attacks. North Korea denied the charges and, as with other similar cases, there is essentially no legal recourse.

Facing the Music

Yet another controversial area is publishing and copyright law. It is no secret that the Internet makes it ridiculously easy to share music, movies, books, and software. Hackers routinely break encryption codes and once something is posted on a peer-to-peer network it often goes viral within hours. There's essentially no way to put the toothpaste back in the tube.

"Modern computer and communications technologies have pushed the law far beyond what it was intended to address," states Andrew Adams, professor of information ethics at Meiji University. "We're trying to make laws designed to apply to industrial middlemen and a 20th century business model relevant for a digital society. This tension is playing out in the legal and political arena with growing frequency."

The music industry is an example of how industrial- and digital-age models conflict. In the early 2000s, record companies resisted selling digital tracks and instead tried to stamp out file-sharing applications such as Napster. When the industry—essentially the Recording Industry Association of America in the U.S.—began serving lawsuits to those suspected of illegally sharing music (some of whom were grandmothers and children) a backlash emerged. Also, "the industry realized that if you sue 100 people and 100,000 people engage in the act, you're never going to catch up to the problem," Adams says.

To be sure, the dynamics of the business, largely as a result of the Internet, had changed radically. This ultimately forced the music industry to adapt to digital distribution of

Milestones

Computer Science Awards

The U.S. National Science Foundation, ACM, IEEE, the Institution of Engineering and Technology, and the University of Exeter recently honored leading computer scientists.

U.S. PRESIDENTIAL AWARD FOR SCIENCE MENTORING

USACM member Juan E. Gilbert, chairman of the College of Engineering and Science's Human-Centered Computing Division at Clemson University, was among nine individuals and eight organizations named as recipients of the U.S. Presidential Award for Excellence in Science, Mathematics and Engineering Mentoring.

ACM GORDON BELL PRIZE

A research group from RIKEN, the University of Tsukuba, the University of Tokyo, and Fujitsu Limited were awarded the ACM Gordon Bell Prize in the peak performance category for execution for their research results obtained using the K computer. The award-winning results, presented at SC11, calculated the electron states of silicon nanowires, which have attracted attention as a core material for next-generation semiconductors.

SEYMOUR CRAY COMPUTER ENGINEERING AWARD

IEEE Computer Society presented Charles Seitz, an architect and designer of innovative computing and communication systems, with the 2011 Seymour Cray Computer Engineering Award in recognition of "innovations in high-performance message-passing architectures and networks."

FARADAY MEDAL

The Institution of Engineering and Technology awarded the Faraday Medal, its most prestigious award, to Donald E. Knuth, professor emeritus at Stanford University's computer science department, for his contributions to computer science.

LOEBNER PRIZE

AI programmer Bruce Wilcox and his new chatbot, Rosette, won the Bronze Annual Medal in the 21st Loebner Prize Competition held at the University of Exeter. It was the second consecutive year that one of Wilcox's chatbots won the Loebner Prize.

content and eventually drop digital rights management protection. The latter, according to Adams, created an additional problem of antagonizing the vast majority of honest content licensees who desire access to their music across their own digital devices. However, while these events were unfolding record companies watched revenues implode. Forrester Research reports that music industry revenues declined from $14.6 billion in 1999 to $6.3 billion in 2009.

Content providers have not given up. Instead they have intensified lobbying efforts. In France, the HADOPI law, enacted in 2009, created a three-strikes procedure that can cut off Internet access for an IP address after repeated copyright violations. In the U.K., the Digital Economy Act 2010 created regulatory code that requires Internet service providers to track and report violations, which could result in penalties, including termination of services.

But the battle lives on. The United Nations recently declared laws with graduated three-strikes provisions a violation of international law. "The level of surveillance needed for applying these rules on shutting down people's Internet connections may be incompatible with EU data-protection rights," says Adams.

Courting Consensus

Amid the chaos, there is a growing effort to create intentional cooperation in the battle against cybercrime. The most visible initiative is the Council of Europe's Convention on Cybercrime, which attempts to join "numerous stakeholders from around the world," including nation-states, nongovernmental organizations that manage Internet resources, business organizations, computer scientists, and Internet users, Kleissen explains.

"Modern computer and communications technologies have pushed the law far beyond what it was intended to address," says Andrew Adams.

Thirty-one nation-states, including the U.S., are parties to the convention, while 16 states have signed the agreement. It provides minimum standards for violations revolving around infringement of copyright, computer-related fraud, intellectual property theft, hate crimes, and violations of network security. Unfortunately, Russia and China haven't signed the agreement. And some criticize the convention for falling behind current threats, including botnets, spam, identity theft, and terrorist use of the Internet.

In the end, perhaps only one thing is clear: The years ahead will present enormous challenges. An increasingly globalized and interconnected world translates into growing concerns over online crime. "Jurisdiction may sound like a technical and dusty issue," Kleissen says, "but without properly functioning rules on jurisdiction, the Internet cannot fully develop to its potential. People must have a reasonable expectation of security and privacy." C

Further Reading

Jaeger, P.T., Lin, J., Grimes, J.M., and Simmons, S.N.
Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing, *First Monday: Peer-reviewed Journal on the Internet 14*, 5, May 4, 2009.

Jurich, J.P.
Cyberwar and customary international law: The potential of a bottom-up approach to an international law of information operations, *Chicago Journal of International Law 9*, 1, July 2008.

Mehra, S.K.
Law and cybercrime in the United States today, *American Journal of Comparative Law 58*, Supplement 1, June 2010.

Marion, N.E.
The council of Europe's cyber crime treaty: An exercise in symbolic legislation, *International Journal of Cyber Criminology 4*, Issues 1 and 2, Jan.–July 2010 and July–Dec. 2010.

Moore, T. and Clayton, R.
The economics of online crime, *The Journal of Economic Perspectives 23*, 3, Summer 2009.

Samuel Greengard is an author and journalist based in West Linn, OR.

Internet

Americans and Social Media

Why do Americans use social media? Mainly to stay in contact with the people who matter most to them, according to a new report from the Pew Research Center's Internet & American Life Project.

Two-thirds of the 2,277 adults surveyed by phone in April and May 2011 use social media platforms such as Facebook, Twitter, MySpace, and LinkedIn, and about the same portion of those social media users say staying in touch with current friends and family members is a major reason they use these sites.

Half of the social media users say connecting with old friends that they have lost touch with is also a major reason. Other factors play a much smaller role. For example, 14% of users say connecting with people around a shared hobby or interest is a major reason they use social media, and 9% say making new friends is equally important.

The ability to read comments by public figures such as politicians, celebrities, and athletes does not come into play as a major factor. Three-quarters of users say this plays no role in their decision to use these sites.

Compared with older adults, social media users under the age of 50 are more likely to say the tools help them keep up with existing friends and reconnect with old ones. About 70% of users under 50 say staying in touch with current friends is a major reason they use online social platforms.

"The most significant finding is that for most users, social media is seen primarily as a tool for maintaining existing key ties," says Aaron Smith, senior research specialist at the Pew Research Center and author of the report. "Activities such as meeting potential dating partners or interacting with public figures are much less relevant than deepening bonds with those who are already important."

—Bob Violino