It's risky and sometimes tough being a top-level file sharer these days. With names such as 'Operation Site Down' and 'Operation Digital Gridlock,' U.S. federal and state authorities, along with European and Asian authorities, are seriously pursuing large numbers of super uploaders, along with organized criminal conspiracies that enable the sharing of copyrighted movies, music, and software, and even thousands of small-time, run-of-the-mill music downloaders.

David Fish, Chirayu Patel, William Veyna, and Nathaniel Lovell, all young men in their late 20s and early 30s, made their first appearance in Federal District Court in San Jose, California, on July 14, 2005. They had all been arrested on felony charges and jailed for violating federal copyright laws, including the Digital Millennium Copyright Act (DMCA) of 1998 and the No Electronic Theft Act (Net Act) of 1997. They are looking at a maximum of five years in federal prison for first offenders under federal sentencing guidelines. They may get more because they were engaged in uploading music and movie files and large-scale distribution and copying (more than ten copies were being made). They were ensnared, along with hundreds of others across the United States and Europe, in a coordinated law enforcement effort to identify, arrest, prosecute, and jail large-scale, organized uploaders of stolen, copyrighted movies, music, and software programs.

Fish and his buddies were members of a Warez group. Pronounced "wares," Warez groups are organized groups of hackers and computer buffs who specialize in capturing copyrighted movies and other digital goods by cracking security codes on CDs and DVDs, or videocamming movies in theaters, and then uploading them to super-servers owned by members of the group. From there, the works can be distributed by local members to friends and relatives, sold to others once recorded back to DVDs or CDs, and in some cases posted to file-sharing networks. There are hundreds of Warez groups on the Internet, and their motive is increasingly to make a profit in stolen works by sharing among group members to hidden servers, and then re-selling to larger audiences.
Warez groups have specialists such as "suppliers" who are able to obtain access to digital copies of works prior to release; "crackers" who use their technical skills to circumvent copy-protection schemes; "cammers" who videocam movies in theaters; and "couriers" who distribute the stolen files to a release network. A release network is composed of large servers owned by members of the group around the globe where the files are stored. From there, the movies, music, and software is re-cut back onto CDs and DVDs and sold or distributed to file-sharing networks without any charge.

This is not your "little boys and friends downloading a few songs on Daddy's computer" story, or even "thousands of students on a single college campus downloading thousands of songs in a semester" story. Rather, this is the story of an organized global criminal conspiracy that accounts for most of the millions of uploaded stolen music, movie, and software files on the Internet. This is a supply-chain story that helps explain how much stolen material gets onto the Internet in the first place. For example, the FBI shut down the Elite Torrents network in May 2005, charging it had permitted 2.1 million files to be downloaded, including 18,000 movie downloads. Over 10,000 copies of George Lucas's movie Star Wars were downloaded from the site in the space of 24 hours in 2004.

Fish and others caught up in Operation Site Down in 2005 were charged with felony violations of the Net Act and DMCA (Digital Millenium Copyright Act). The Net Act makes it a federal felony offense to reproduce or distribute copyrighted works even if there is no profit motive. Ten or more copies makes the offense a criminal felony. The DMCA makes it a felony offense to break a digital copyright protection scheme.

While federal and international authorities have focused on the organized uploaders of stolen digital works, the Record Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) have been active at the other end of the spectrum of file sharing: the small-time downloader at home or on campus, who downloads a few songs a week or several thousand over a year's time. For these individuals, the risks are also rising. The RIAA has filed over 15,000 lawsuits against individuals for illegally downloading and distributing copyrighted music. In about 3,400 of the cases, the defendants settled, and paid the RIAA a fee averaging between $4,000-$5,000. The rest are pending. The MPAA has filed over 300 lawsuits against individual downloaoders, and larger super-sites that store uploaded movies prior to distribution to file-sharing networks. The MPAA follows the same procedures pioneered by the RIAA after illegal music trading: first, intercept the Internet address of a person sharing a movie on a peer-to-peer network and then sue them as an unidentified "John Doe" defendant in a federal civil case. The MPAA can then subpoena the ISP to reveal the person's name, allowing the person to be sued individually for damages. Generally, copyright law puts a price of $30,000 on each film infringement, or up to $150,000 if it is deemed willful.

While law enforcement and industry groups scramble to find legal tactics for preventing large-scale theft of their content, the amount of file sharing and downloading of copyrighted material has continued to grow, although not as fast as in the past. Meanwhile, legitimate sources for online music and film, such as Apple's iTunes online music store, RealNetworks Rhapsody subscription network, and movie sites such as CinemaNow, MovieFlix, and Movielink are experiencing double-digit expansion.
CHIEF PRIVACY OFFICERS

How can you tell if your own corporate practices actually conform to the privacy policy stated on your Web site? How can your business keep track of all the new privacy legislation and changes in European policies? The answer for many corporations is to create a new executive position—Chief Privacy Officer (CPO). Firms such as IBM, AT&T, Eastman Kodak, DoubleClick, New York Life, ChoicePoint, and many others have recently added this new position to senior management ranks. According to Information Security magazine, the CPO position is one of the fastest-growing in corporate management. There are now over 2,000 CPOs in the United States, compared to 350 in 2001, according to Alan Westin, founder and president of Privacy & American Business, which runs a training program for CPOs. But that's still nothing compared to Europe, where Germany has 2,000 data protection officers alone.

What does a CPO do? According to Richard Purcell, formerly CPO for Microsoft, the job has three aspects: coming up with privacy policies for the firm to follow, monitoring the development of new technology to ensure it respects consumer privacy, and informing and educating the company's employees about privacy. Another job is helping the company avoid privacy "landmines," which are mistakes in policy or technology that, had any one thought about it, would obviously be embarrassing to the company because of the potential for a storm of protest from privacy protection groups. For instance, in 2005, IBM's CPO proactively led the fight within the company to ban the use of genetic data in the employment recruiting and promotion process. AOL proactively changed its privacy policy for the first time since 1998 by stopping the practice of selling mailing lists to retailers, and stopped using information from advertising networks and non-AOL sites to customize ads. In other cases, in the absence of a CPO, disaster is possible. U.S. Bancorp decided to sell personal financial data to a direct-marketing company in violation of its own stated policies. This cost Bancorp $3 million in a legal settlement in Minnesota. RealNetworks had to apologize to users and change its data collection policies after a disclosure that the company's RealJukebox Internet music software captured data about users' preferences. In 2005, a string of data losses, criminal intrusions, and accidents at data brokerage firms such as ChoicePoint and Reed Elsevier's LexisNexis unit resulted in the diversion and theft of hundreds of thousands of complete personal profiles. This in turn has led to Congressional investigations, fines, and the threat of restrictive legislation for the entire data brokerage industry.

The new corporate emphasis on privacy has also created a new business for the big accounting firm PricewaterhouseCoopers as one part of its Global Risk Management Solutions. PWC has conducted hundreds of privacy audits. Companies are taking this issue very seriously because data theft or loss and invasions of privacy directly threaten the brand names of firms. Privacy audits identify the risks that firms face and prescribe corrective actions with a view to avoiding class action suits, Internet-based protests, and shareholder enmity. And what do the auditors find? About 80% of the companies audited by PWC do not follow their own stated privacy policies. Most of the time this is the result of poor training and human error.

(continued)
After Expedia completed a privacy audit led by PWC, it changed its information collection policy from opt-out to opt-in. Now Expedia’s customers have to actively click a button and ask to be informed of new offers from the travel site. The result is that far fewer customers ask to unsubscribe from mailing solicitations. Expedia executives believe trust and privacy are major concerns of their customers, and anything they can do to enhance trust is good for their business.

What do CPOs worry about? They often have a hard time with their own employees taking privacy seriously and changing policies to cope with the risks. In the case of ChoicePoint’s loss of 145,000 personal dossiers to criminals posing as real companies, ChoicePoint has hired a CPO who reports directly to the Board of Directors and the CEO, and has changed its procedures for verifying the authenticity of people claiming to be legitimate businesses. Prior to this breach of its database, ChoicePoint did not verify the authenticity or legitimacy of people claiming a business need to access their databases.

Perhaps the biggest challenge facing CPOs is federal legislation that requires companies to inform consumers of their privacy policies, and the trend away from a pro-active, pro-consumer privacy officer and towards a narrow legalistic emphasis on compliance. The Graham-Leach Bliley Act of 1999 requires all financial service firms to inform consumers of their privacy policies. This results in tens of millions of pamphlets being sent to consumers, often written in confusing legal jargon that few can understand. HIPAA, designed to make the transfer of records among health care agencies more efficient as well as to safeguard the privacy of those records, has also unleashed a flood of privacy pamphlets that few can understand. HIPAA requires that all health care providers and insurers have a privacy officer, even in small medical practices with seven doctors. Professional associations such as the International Association of Privacy Professionals openly worry that legalistic compliance with federal laws fails to take into account the real interests of consumers and the strategic implications for the firm.


PRIVACY ADVOCACY GROUPS

There are a number of privacy advocacy groups on the Web that monitor developments in privacy. Some of these sites are industry-supported, while others rely on private foundations and contributions. Some of the better known sites are listed in Table 9.9.
THE PRIVACY TUG OF WAR: ADVERTISERS VS. CONSUMERS

We are in a technological tug of war between technologies that make invading customer privacy very easy versus other technologies that make protecting privacy easier. On the privacy invasion side, Experian.com links Web sites to its database and provides the names and addresses of visitors to the sites in real time. Other companies such as Axcion.com combine offline and online purchasing and behavioral data into one central database. Network advertisers place tracking cookies on your computer whenever you visit a member site and these cookies report your subsequent movements and are used to select ads you will be shown. Meanwhile, you have to be very careful not to open e-mail attachments or click on a promise of “instant rewards” on a Web site lest you accidentally download and install a spyware or adware program that will either be used to track your every keystroke or, more benignly, to swamp your screen with ads you never wanted to see in the first place.

How do the advertisers justify their intrusions into our private use of the Internet? The answer is profoundly interesting. Here’s the idea, according to senior executives at advertising networks such as DoubleClick: the implicit bargain underlying the “free” Internet is that consumers get content because they are looking at ads. Never mind that you paid around $1,000 for the PC, and $30–$50 monthly for Internet service. Take away the ads, and some other way will have to be found to pay for what you get on the Internet. The other main rationale behind all these intrusive behaviors is marketing efficiency and effectiveness: the more advertisers know about you, the more they can customize and personalize the advertising to exactly what you are looking for at right time, and, of course, the more they can charge their customers, the firms that pay for the advertising. Online advertisers believe consumers are saying “Take my privacy, but please send the content.”

The problem is that most consumers don’t really accept this deal. It’s possible that the advertisers don’t know the consumer very well. A recent industry-backed survey of over 1,000 Web users found that only 14% said they liked giving information to Web sites in order to receive customized content, and 71% said they disliked it but did so only if necessary to obtain content or information. Forrester Research reports, for instance, that 42% of shoppers cut back Web purchases in 2005, causing a 1% to 3% fall off in the rate of e-commerce growth. Consumers seem to be saying “Send the content, but let me keep my privacy!”

On the privacy protection side, there are a great many more tools available to consumers than just a few years ago. Admittedly, P3P, an industry-sponsored effort to provide users some choice in privacy by making them aware of Web site privacy policies, has not been too successful. But ISPs and independent software companies now provide a host of tools that work wonders and are easy to use. For instance, iPrivacy.com provides a tool called SurfGuard that deletes cookies, pop-ups, in-line ads such as banners, and executes (literally) any spyware program, all for $29. Web sites such as AOL.com, MSN.com, and Yahoo.com have similar tools for subscribers. The open source browser Firefox and new versions of Internet Explorer have effective pop-up and image blockers. Anti-spyware programs in particular are now adopted by over 80% of Web users and over 40% report regularly deleting (continued)
cookies, especially third-party cookies used by ad networks. Adoption rates of cookie blockers and anti-spyware software is increasing as software makers such as Symantec make them available as a part of their software suites that install automatically. Even if these estimates are off by 50%, a significant number of ads are not actually being shown to consumers.

All these consumer self-help activities have traditional Web advertisers worried. What if consumers rejected the idea of pop-up ads, tracking their behavior, and storing all this information about them? What if consumers did not buy into the "free Internet with ads" deal? What if 50% of Internet users adopted ISP-provided privacy protection or bought their equivalents on the market? While Internet advertisers have pretty much blocked effective legislation in Washington that would preserve privacy, and while their industry associations have quite clearly failed to bring about meaningful self-regulation, the market has responded by providing consumers with some powerful tools for protecting their own privacy. Perhaps the success of Google's advertising model, which prohibits pop-ups, streaming Flash animations, and banners but allows silent text ads confined to little boxes, lies in the fact that these ads don't bother consumers so much.


---

INTELLECTUAL PROPERTY RIGHTS

Congress shall have the power to "promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."

—Article I, Section 8, Constitution of the United States, 1788.

Next to privacy, the most controversial ethical, social, and political issue related to e-commerce is the fate of intellectual property rights. Intellectual property encompasses all the tangible and intangible products of the human mind. As a general rule, in the United States, the creator of intellectual property owns it. For instance, if you personally create an e-commerce site, it belongs entirely to you.
THE INTERNET DRUG BAZAAR

In May 2005, federal law enforcement officials seized $18 million in assets from Christopher Smith, a 25-year-old Minnesota man whose online prescription business had been under investigation by federal authorities for four years. No criminal charges were filed, but he and his 85-person company were accused of defrauding consumers, and distributing prescription drugs without appropriate prescriptions, and violating a host of federal and state laws. Smith was also charged with being America’s most prolific spammer, sending more than 1 billion spam messages through AOL alone in 2005. Despite occasional crackdowns, online prescription drugs and pharmacies are one of the fastest-growing business models, and oddly, senior citizens—some of our most law-abiding citizens—are leading the charge for cheaper drugs.

In 2005, online pharmacies accounted for over $1 billion in revenue. Overall, online health spending for the year was projected at $2.9 billion, with about $1.3 billion of that for online pharmaceutical drugs. Business is good at online pharmacies, with an estimated 21% annual growth. No one knows for sure how many online pharmacies there are, but a Food and Drug Administration report in 2005 identified over 11,000 online pharmacies that purported to be Canadian companies. However, only about 1,000 of these sites actually sold drugs; 86% were hosted in the United States, and 70% were registered to U.S. owners. The main attraction of online drug sites is price. Typically, they are located in countries where prescription drugs are price-controlled, or where the price structure is much lower, such as in Mexico. U.S. citizens can often save 50%–75% by purchasing from online pharmacies located in other countries.

The problem is that, according to the 1938 Food, Drug, and Cosmetic Act, prescription drugs may not be bought without the involvement of a physician, and must be dispensed by a state licensed pharmacy. However, e-commerce has challenged this traditional method of controlling medicines that can kill people if they are not properly dispensed and supervised. For instance, anabolic steroids, prescription diet drugs, Viagra, and narcotic painkillers—all potentially dangerous and life-threatening—are freely available on the Internet without a prescription. Instead, many online pharmacies use questionnaires to diagnose disease and supposedly have these questionnaires reviewed by doctors. So-called “consulting physicians” will write you a prescription online. In one case, a journalist used the name of her cat when ordering drugs and received just what she wanted. In some cases, Internet pharmacies are fly-by-night operations dispensing counterfeit drugs.

However, not all Internet pharmacies are illegitimate. According to the FDA, there seem to be about 300 that require a real prescription. In fact, all of the Canadian online pharmacies in the FDA study actually located in Canada and belonging to Canadian citizens did in fact require a prescription. Most of the troublesome online sites were located or owned by people in the United States or other countries, such as Australia, the Czech Republic, El Salvador, Germany, Mexico, and Vietnam. So what do you get when you order online, especially from the offshore sites in Europe, Asia, or Latin America? The Government Accountability Office (GAO), a research arm of Congress, conducted a study of online pharmacies in 2004. GAO placed 90 orders at 68 Web sites (some U.S., and other foreign) for 13 prescription drugs. The most common problem was not receiving any drugs—22 (continued)
orders were never filled at all. Other problems included no instructions for use (23 samples) and no warning information (21 samples). But only four samples contained counterfeit drugs.

The federal government plays a role in regulating prescription medicine, but states play a much larger role in licensing physicians and pharmacies. The Food, Drug, and Cosmetic Act provides that prescription drugs cannot be sold without the involvement of a physician, and gives the FDA authority to enforce that provision. However, the FDA has been slow to respond to the e-commerce sales of prescriptions or to investigate the extent of the problem. While pharmaceutical companies push for strong federal legislation to make importing of drugs from low-cost countries such as Canada or Europe illegal, state governors and mayors, and some corporate health officials, are setting up Web sites to help their citizens and employees buy drugs from reputable Canadian sites. A very vocal and politically powerful group called “senior citizens” is in favor of unrestricted online sales: 37% of visitors to online Web sites in 2005 were over 55 years of age. The result is a political stalemate.

So far, Congress has not passed any legislation regulating online diagnosis or prescription drug sales. Consumers could be purchasing from foreign sites and not know it, and they also could be purchasing bogus medicines. In this environment, the FDA urges consumers to check with the National Association of Boards of Pharmacy (Nabp.net) before purchasing any prescription drugs from an online pharmacy.