Many privacy laws can be applied to medical records

Imagine a system in which access to data is limited to proper people

In an essay portending massive challenges to copyright law from the Internet—if only because merely viewing information online entails, as a technical matter, making a copy of it—Temple Law Professor David Post retells the story of three eras of publishing, the latest ushered in by the Internet:

■ Era of Monastic Manuscript: Copyright unnecessary to authors or publishers.

■ Era of Gutenberg Press: Copyright necessary to authors and publishers.

■ Era of Promiscuous Publication: Copyright enforcement doubtful.

Until recently, the music industry has feared ruin from the unauthorized swapping and rebroadcasting of high-quality audio reproductions among its customers, a phenomenon enabled by increasingly cheap networks, data storage, and processors—again, the Era of Promiscuous Publication.

The music industry has found recourse to law largely unavailing against this tide of technological progress. The industry is embarking on a different strategy—changing the technology itself.

At the core of the technological response lies the idea of "trusted systems": computer databases of the rights and privileges of specific entities vis-à-vis information, linked to hardware and software that recognize and enforce those rights. If fully deployed, trusted systems could trump the Era of Promiscuous Publication with what I call an "Era of Trusted Privication," one in which a well-enforced technical rights architecture would enable the distribution of information to a large audience—publication—while simultaneously, and according to rules generated by the controller of the information, not releasing it freely into general circulation—privication.

What can the publisher teach the patient? I believe trusted systems technology, bearing much promise for the control of intellectual property, can separately help vindicate medical records privacy interests online.

The music industry response

The publishing industries initially responded to the Internet boom, and the corresponding surge in illicit copying of their wares, by using their political power to broaden and strengthen the scope and application of copyright law. However, as it became clear that the problem would not be overcome by additional difficult-to-enforce legal rules, the music industry has turned to technology backed by law as a more promising avenue for redress.

An examination of each of these types of responses, legal and technical, yields possible ways that privacy advocates can benefit from the lessons of the music industry's experience.

The technological premise behind trusted systems is simple but contrarian: The Internet of today is what we have made it—and the Internet of tomorrow will be whatever we remake it to be. Each need not bear much resemblance to the other.

The cliché that the Internet "recognizes censorship [and presumably information blockage from any source] as damage and routes around it" has perhaps prematurely achieved the stature of truism.

With medical privacy, individuals are seeking protection against well-organized corporate interests.

How could a future Internet realistically tame the current information chaos? Mark Stefik, a researcher at Xerox PARC, has been quietly developing and touting an answer for several years.

Stefik is among the leading architects of so-called "trusted systems," technological gatekeepers that allow "authorized" flows of information while flatly blocking "unauthorized" uses. A necessary element is the ability to structure "rights" into a calculable framework that is then automatically enforced by the technology. The system can be said to have "trust" to the extent that these rights architectures are made secure—when, through a combination of hardware and software, a user who is anything less than a talented hacker is truly constrained by the system at the behest of whoever is the source of the information it might display.

A trusted system can be trusted by a rights-holder as against the user of the system—even if the physical system is in the custody of the user.

Trusted systems comprising computers linked by cheap, fast (perhaps wireless) networks could enable the following hypothetical world of commercial music: Songs are not "sold" in even the colloquial sense of the word; rather, they are "licensed"—from a legal and technical standpoint. Compact discs can join 8-tracks, cassettes, and phonograph records in the dustbin. Their replacements are small, generic "jukeboxes" linked by the Internet to a central repository of songs managed by a publisher.

A female student may authenticate herself to a jukebox—perhaps with a fingerprint—and then may access songs that fall under her monthly payment plan.

The songs she asks for are "streamed" to her player as she listens, and do not remain there any more than a song stays inside a radio after it ends.

An inaudible signal is embedded in the music; if she holds a microphone to her headphones and makes an imperfect, analog copy to an old-fashioned cassette, her name and a unique identifier will be "in" it, permitting prosecution for copyright infringement.

If she were to abuse her access to the system by hooking up her jukebox to an amplifier for a beach party, a cheap listening post on the beach's lifeguard chair, monitored by ASCAP, would use a watermark decoder to determine instantly that she was behind the cacophony—and that the particular performance had only been paid for at the "portable personal use" rate rather than the "noncommercial party" rate.

A more likely event is that she will fall behind in her monthly payments, in which case her access to any music—except that which is heard over old-fashioned analog "public" radios—will be cut off automatically.

A world like this is still at least 5 years off by my conservative reckoning—and the music industry may elect not to invoke all the technical power that could be at its disposal. Still, publishing industries have already taken the first halting steps toward trusted systems architectures.

The ambition of this technical strategy is to hasten a new era (or perhaps take us back to an earlier one) before the current one has truly settled in. We might revise Post's timetable as follows:

■ Era of Monastic Manuscript: Copyright unnecessary to authors or publishers.

■ Era of Gutenberg Press: Copyright necessary to authors and publishers.

■ Era of Promiscuous Publication: Copyright enforcement doubtful.

■ Era of Trusted Privication: Copyright unnecessary to authors or publishers.

The term "privication" is meant to capture the heretofore unlikely coupling of mass distribution of information to authorized users with tight control over its use—at least along the dimensions of perfect, instantaneous, and anonymous copying. That control is enabled through private not public means, eliminating the need for copyright.

Securing medical records

The elements of the information technology revolution that worry intellectual property holders carry parallel significance for individuals as personal data holders. After all, whether for profit or dignity, each group desires the same end: control over information.

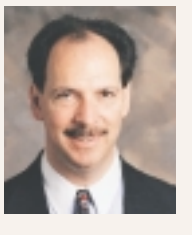
There is, however, a fundamental shifting of roles. In the context of intellectual property, it has mostly been well-organized corporate interests seeking protection against death by "little guy" information pirates. With medical privacy, individuals are seeking protection against a whittling away of privacy by well-organized corporate interests.

More than one commentator has lamented that video rentals have more emphatic federal protection than medical data. This is so despite the rapid digitization of sensitive medical records, a marked increase in the amount of in-

SEE PRIVACY ON PAGE 14

author info

Jonathan Zittrain is assistant professor of law and co-founder and faculty co-director of the Berkman Center for Internet & Society at Harvard Law School, Boston. Readers may contact him at *zittrain@law.harvard.edu*.



H. Jay Wisnicki, MD, editor of Tech Talk, is the head of the ophthalmology department at Beth Israel Medical Center in New York. He has a background in computers and electrical engineering. He serves on the AAO New Education Technology Committee and advises in other areas in health-care information technology.

PRIVACY
Apply to medical records

CONTINUED FROM PAGE 10

formation a "medical record" now comprises, and a number of "scare stories" about misuse of medical data.

Congress formally ushered in the networked era for medical records in 1996 when it passed the Health Insurance Portability and Accountability Act. The act's "administrative simplification" provisions were intended to assist the health-care industry in standardizing electronic formats for medical records, ultimately by having the government mandate certain technical standards derived from the private sector. Some standards have already been generated through this process.

The law also set an August 1999 deadline for Congress to come up with privacy restrictions to complement the technical standards for electronic medical records. Congress missed its deadline, and the law required that the Secretary of Health and Human Services (HHS) impose such standards in its stead. The secretary's draft regulations were put out for public comment in November 1999 and were approved by then President Clinton in December 2000.

The draft regulations entail substantive enhancements to privacy rights combining the fiat of rule-and-sanction regulation with a dash of strengthened contract-like rights. For example, health organizations may not release medical records that are easily identifiable unless certain specific exceptions apply.

Further, patients are given the right to inspect their own records. No private right of action is contemplated for violation of any of the rule's proscriptions. Identifiable data may be released for virtually any otherwise lawful purpose with a patient's consent, and the rule goes into great detail about how that consent should be obtained, featuring a number of mandatory disclosures and a requirement that consent be revocable.

These rights, however, aren't easy to assert in practice: HHS has admitted the difficulty of managing claims of abuse of patient data, not to mention the difficulty of discovering such abuses.

Perhaps a trusted system could help.

First, so long as permissible and impermissible information practices can be defined in a way satisfactory to most interests—to be sure, a daunting challenge—consumers of medical data might well prefer an architecture where it is, as a technical matter, difficult to stray from authorized uses. The implementation of the trusted system could be a safe harbor defense against a class-action suit, agency enforcement proceeding, or other litigation-dependent remedy.

Second, privication architectures might help meet the daunting challenge of defining fair information practices, since the increased granularity of rights afforded by a technological system makes room for entirely new rights constructs. To explain: The expression of rights through a trusted system may allow for "baby-splitting" among interests that is not feasible in more traditional regimes. For example, in place of the stalemate over who should "own" a record, a well-defined self-enforcing rights architecture could allow information sharing without ultimately having to resolve matters in a coarse way as "owner" and "nonowner."

A patient might wish to have the right to delete his or her records, while medical researchers would object to the nonrandom loss of possibly important medical data. The system could enable deletion for "most intents and purposes"; one could imagine a deleted record no longer appearing on a hospital computer display or being available for marketing purposes, while still being available for medical researchers.

Just as a musical trusted system might distinguish between students and businesspeople—to enable price discrimination by the publisher—a medical trusted system might distinguish among the identities of those seeking to use the system. Indeed, the easy unbundling of songs from an album in the music context could become the unbundling of some data elements from others in patient records.

A patient could release maternity information for marketing purposes while withholding HIV status; the government could still access the entire record (with process) for subpoena purposes if the entire record were deemed relevant, but otherwise it too could get only the information needed for a particular purpose, such as payment information for fraud reduction efforts.

For audit rights, a patient might be able to see everything in his or her record except that which is explicitly marked to be held back by an authorized doctor. Then, at least, he or she would have a sense of what he or she did not know and why, and his or her access to some parts of the record would not be held hostage to other parts. All this could be done with a minimum of administrative burden on the database custodians.

Allowing granular "dynamic consent" for medical data could see patients electing to accept offers of all kinds for releasing their information, creating market efficiencies for the sale of vertically integrated patient information where before there was primarily only the release of horizontally integrated data by health care institutions.

As various databases begin to converge—imagine the use a doctor could make of data on everything from one's genome to one's supermarket purchases to correlate diet with a given disorder—an ability to set sophisticated gates efficiently around data elements could be critical.

Finally, trusted systems' Newtonian inertia of rights enforcement will help medical privacy interests over the long term given their weak political representation and power. Once the system is in place, government cooperation is not nearly as important as it might be to traditional rights enforcement.

The recent expansive history of federal copyright protection may well cause us to underappreciate this point, since the music industry has enjoyed an ongoing application of government protection and pressure to vindicate its rights before beginning to turn to trusted systems. Federal privacy protection, on the other hand, has more closely resembled the booth at the county fair where one attempts to swing a hammer so hard as to ring a bell overhead: It happens rarely, and the resonance fades not long after the deed is done.

It does happen from time to time, however, and if the pressure that brought about federal privacy protection for video rental and driver's license records can be brought to bear for medical records in one concentrated swoop as the Department of Health and Human Services maps out privacy-protection regimes through its rulemaking, the trusted system might be established and then resonate much longer thanks to its momentum.

In a political environment marked by persistent stalemate, the conception of a privication architecture for medical records could encourage new compromise among formerly competing interests, and ultimately more privacy protection with a minimum of social cost.

Strele manages Zeiss Humphrey global business

FROM STAFF REPORTS

DUBLIN, CA—Carl Zeiss Ophthalmic Systems Inc., Humphrey Division, has appointed Jean Robert Strele to vice president, international business. Strele previously held the position of director, international business for the company.

In his new role, Strele will manage Humphrey's international business including identifying and developing international distribution channels.

"Our strategy is to develop our distribution channels further throughout the world to maximize market penetration," Strele said.