Stanford Law Review
May, 2000

Symposium
Cyberspace and Privacy: A New Legal Paradigm?

*1201 WHAT THE PUBLISHER CAN TEACH THE PATIENT: INTELLECTUAL PROPERTY AND PRIVACY IN AN ERA OF TRUSTED PRIVICATION

Jonathan Zittrain [FNa1]

This article begins with a premise that intellectual property and privacy have something significant and yet understated in common: both are about balancing a creator's desire to control a particular set of data with consumers' desires to access and redistribute that data. Both law and technology influence such balancing, making it more or less palatable to use data for particular purposes--whether one is an individual making a copy of a popular song for a friend, or a hospital selling a list of maternity ward patients to a day care service. In the shadow of the Internet's rapid development and concomitant easing of barriers to data sharing, holders of intellectual property are pairing increased legal protection with the technologies of "trusted systems." I describe how these technologies might allow more thorough mass distribution of data, while allowing publishers to retain unprecedented control over their wares. For instance, an e-Book seller might charge one price for a read-only copy that could not be printed or forwarded and charge an additional fee for each copy or printout made. Taking up the case of medical privacy, I then suggest that those who worry about the confidentiality of medical records, particularly as they are digitized by recent congressional mandate, might seek to augment comparatively paltry legal protections with trusted systems technologies. For instance, a trusted system could allow a patient to specify how and by whom her records could be used; within limits, she could allow full access to her primary care physician, while allowing only time-limited access to emergency care providers, non-personally identifiable access to medical researchers, and no access at all for marketing purposes. These technologies could allow for new kinds of privacy protection, without sacrificing the legitimate interests of the consumers of medical records.

*1202 Introduction

Individuals have long had the desire but little ability to control the dissemination of information about their health. Law has been a weak instrument for such control, given the articulate and powerful interests that insist upon maintaining and enhancing access to others' personal information, with access to sensitive medical data proving only a sporadic exception. Technology has so far only made exploitation of personal information easier. The evolving federal framework for the protection of medical records likely will make individuals the third-party beneficiaries of flexibly interpreted, ponderously enforced fair information practices created in the shadow of a congressionally mandated networking of sensitive medical data. This networking promises to lower greatly the costs of accessing and using medical data for any number of purposes--including ones not central to health care, such as direct marketing. It is ushering in what some call the "Era of Promiscuous *1203 Publication." [FN1] The danger this era portends is that what is gained in efficiency of health care provision may be lost in erosionof privacy. Privacy advocates could learn a new approach to this problem from an unlikely teacher: publishers of intellectual property--specifically the American music industry.

The music industry until recently feared ruin from the unauthorized swapping and rebroadcasting of high-quality audio reproductions among its customers, a phenomenon enabled by increasingly cheap networks, cheap data storage, and cheap processors--again, the Era of Promiscuous Publication. Despite access to a sympathetic Congress and extensive enforcement resources, the music industry has found recourse to law largely unavailing against this tide of technological progress. The industry is now 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-a-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.

In my view, there is a profound relationship between those who wish to protect intellectual property and those who wish to protect privacy. Their common desire to control the distribution of information, and the music industry's potential success at regaining control through the implementation of trusted systems, offer several lessons to privacy advocates seeking to protect the privacy interests increasingly threatened by the advent of the Era of Promiscuous Publication. I will explore these lessons first by mapping out the problem presented to the music industry by the advent of fast, cheap, and perfect copies, along with the music industry's legal and technological strategies for regaining control. Second, I will describe the similar problem faced by privacy advocates in the arena of medical privacy, the legal solutions that have been and might be attempted, and a hypothetical technological solution that demonstrates the enforcement power of the trusted system. Finally, I will look beyond the enforcement potential of the technological solution to demonstrate how thinking in terms of privication architectures might help negotiate the allocation of rights to medical data to account for the interests of individual "producers" of personal data in ways that need not disparage the legitimate interests of the sophisticated institutional players who wish to consume that data.

* * *

II. Lessons from the Publisher: The Power of Privication Architectures

I now review some of the features of trusted privication architectures that make them distinct from law even as they rely upon it. These features allow publishers to control their work more readily than through law alone, and ultimately point to ways that privacy interests can be better vindicated.

A. Discrimination on the Basis of Consumer Characteristics

Mass publishing has typically by necessity contemplated an undifferentiated market. One cannot distinguish--and price discriminate--among buyers of intellectual property except in quite crude ways. A publisher might attempt a temporal staging of a new book--the more expensive hardcover edition sold to those who are willing to pay more to buy now, followed by a cheaper paperback edition for those who are more price sensitive--but the ready transferability of intellectual property eliminates most other schemes of discrimination. Indeed, the first sale doctrine, by which one legitimately encountering a particular copy of a protected work may lend or resell it without restriction, ensures that most serious attempts to distinguish among buyers can be met with arbitrage. [FN69] Privication can change that, because the systems that enable it can cheaply couple information gathering about a buyer with the quotation of a price, while preventing cheap arbitrage between those who are offered a discount and

those who are not. Thus a student gets access to music at a given ongoing rate but cannot readily attain custody of a "copy" of it that in turn may be transferred or simply copied to another person.

*1222 B. Nuance in Provision of Desired Information

With a trusted system, "access" to a work can have a spectrum of meanings far more subtle and powerful than, say, the binary option of either giving someone a compact disc or not. As the hypothetical future of music distribution described above suggests, unlike traditional publishing, where it is hard to physically dispossess someone of a work after she has bought it, the opportunity to "stream" information--making it available for momentary exposure without giving an actual copy to the consumer--suggests completely new models of information provision with corresponding new metrics of remuneration. A single song can, at the discretion of the publisher, remain a product to be sold and re-sold, or repackaged as a service in which a consumer buys rights to listen to a song for a period of time or a discrete number of plays, after which the rights lapse. Furthermore, songs can be unbundled from one another, no longer forcing publishers to set the boundaries of a given "album."

C. Prevention Rather than Punishment of Undesired Behavior

The effectiveness of traditional "rule and sanction" law as a means of behavior control is a function of its certainty, swiftness, severity, and normative acceptance. The ability of individuals to swap copyrighted music without being readily identified makes the prospect of punishment quite remote, despite a strict law on the books clearly prohibiting the act in question. And while it may be difficult to overstatethe level of government support for strong intellectual property protection, prosecutorial commitment to expending scarce resources to prosecute individual intellectual property crimes is not likely to be strong; so far only "ringleaders" of intellectual property piracy groups have been targeted. Similarly, though the industry has no reluctance to bring private causes of action against perceived infringers, litigation is costly, time-consuming, and poorly calibrated to the small claims at stake in many instances.

Thus, for that part of the problem that bears on enforcement of constraints against multiple small individuals ("elephant vs. gnats"), a privication framework might be a preferable recipe. If the cost of piracy can be increased through significant barriers to breaking a technical architecture that prevents it, rather than a calculus combining the likelihood of being caught with the severity of punishment, control might be more efficiently effected. Put another way: An ounce of prevention is worth a pound of cure; few banks would prefer a solved robbery to a vault never robbed.

*1223 D. "Newtonian" Motion: The Inertia of Trusted Systems' Constraints

A well-constructed trusted system could, once established, maintain its constraints comparatively more cheaply and with less government cooperation than those defined and enforced through a legal regime.

A trusted system could be cheaper because, apart from the fixed costs of designing and deploying it, there are low ongoing costs to its maintenance. This is true in the simple sense that software does not wilt after repeated uses, and if its function is to produce sophisticated gates around information, it can continue to staff them without the annuities necessary for human guards. Trusted systems upstage most of law's enforcement mechanisms, dependent as they are on attorneys general, courts, or legislatures.

Moreover, networked technologies can attain a self-perpetuating momentum; once in place they can be quite difficult to uproot. [FN70] A system intertwining suppliers and consumers exhibits just these network externalities.

The power of market-based network effects reduces the need for continued government backing of the constraint scheme embedded within the network. To be sure, the language used to map out the components and features of a trusted system is the language of law--rights, ownership. These words capture their technical functions while remaining somewhat true to their legal etymology: As with traditional legal rights, they represent the constraints that some users can place on others, constraints from which those others may not readily deviate. Unlike traditional legal rights, however, the constraints designed into most trusted systems--and then invoked by one user against another--are not themselves "legally protected interests." [FN71] Even in the publishing context they are not like copyright, for no legislature defined them, and no court interprets them. They are not like contract, because the assistance of the state is not needed to validate and enforce their terms. [FN72] *1224 They can be at once highly effective and highly independent of government intercession. [FN73]

This may be an easy feature to miss when reflecting upon the publishing industries' intended use of trusted systems, given how little trouble they have had marshaling government support for ongoing rule-and- sanction protection. Still, even a politically advantaged stakeholder would, all else being equal, presumably wish to rely as little as possible on the potentially fickle solicitousness of the public arena toward its interests.

E. Opportunity for New Rights Constructs

The story of trusted systems for publishing so far looks to be one of winner- take-all: The designers of the system tilt each of the features just described to their maximum advantage. In the case of the music industry, we might say that the trustee is computer technology and the companies behind it, and the trusters are ASCAP and BMI. After a rocky start, they are collaborating to ensure that music listeners enjoy their products on the basis of something other than the honor code or the legal code. The untrusted is the public: computer owners at large who might ask their computers to do more with content than the originator of the content would like.

If publishers in a world of trusted privication do not need copyright's protections, its countervailing privileges--already weak--need not be respected. [FN74] Fair use is merely a defense against a claim of copyright infringement; it is not a "right" that one can affirmatively exercise to claim access to data or an ability to copy it. Within the "Trusted Privication" framework, the law's sanctions and exceptions are equally irrelevant, and the issue is only whether the act of copying can be made technically nontrivial. [FN75]

*1225 Because the music industry--the supplier of content--is the predominant force establishing a system of privication, the rights architecture the system reflects might inevitably appear lopsided to consumers of content. This lopsidedness may first appear as simply hyper-enforcement of existing intellectual property law.

However, trusted systems and "privication" are not merely about enforcement, and they need not be lopsided. Indeed, they offer opportunities to create new distributions of constraint and freedom among consumer and producer, ones that need not reflect substantively extreme allocations to one or the other. The quite basic trusted system of a taxicab meter enforces a rule on fare calculation, but it also calculates a fare on the basis of subtle combinations of the distance covered and time spent stopped in

traffic in a way that driver and passenger simply could not--a new, perhaps "fairer" accounting of what a passenger owes a driver than what a glance at an odometer or reliance on a crude geographic "zone" system could provide.

Some implementations of a trusted system could help better reconcile the conflicting interests of consumers in listening to cheap music (and exchanging ideas and speech with one another) with a level of control over work that would satisfy the music industry. For example, one could imagine allowing "fair use" of music so long as it was not at full digital quality--for example, one could listen freely to songs at AM radio quality, while having to pay to hear them at full fidelity. This might or might not make economic sense to the industry, but in any case it could advance the sort of social policies that underlie fair use by allowing everyone, rich or poor, to benefit from listening to music, without endangering the market for music among those who wish to pay for it. A trusted system might provide that elementary school music teachers could play music for their students in the classroom for free, without worry that the students--or teacher--could then take the music home or resell it to others not at school. There could be corresponding new forms of "fair use" for books, articles, speeches, and newspapers. Control might be tightened in some areas, loosened in others.

Unless market forces demand them, these "moderate" systems are unlikely to arise in publishing, at least as long as the industry is building the *1226 system and Congress sees no reason to intervene on behalf of the public interest. But these sorts of new balancing constructs may prove quite important for privacy, where privacy advocates are among the least advantaged at the table of public choice.

III. Medical Data: A Trajectory of Personal Privacy Worries--and Responses to Them--in a Digitally Networked Environment

A. A New Problem: Quick, Cheap, Perfect Copies

Sun Microsystems's Scott McNealy threw down the gauntlet to those who care about privacy in the spring of 1999. His observation was pithier than Barlow's declaration to the information industries, [FN76] if less lyrical:

> "You already have zero privacy. Get over it." [FN77]

The elements of the information technology revolution that worry intellectual property holders carry parallel significance for individuals as personal data holders. [FN78] After all, whether for profit or dignity, at the core each group desires the same end: control over information. There is, however, a fundamental shifting of roles. In the context of intellectual property, worry has come largely from well-organized corporate interests seeking protection against a death by a thousand cuts from "little guy" information pirates. With privacy, worry has come largely from individuals seeking protection against a whittling away of privacy by well-organized corporate interests. [FN79]

*1227 More than one commentator has lamented that video rentals are treated to more emphatic federal protection than medical data. [FN80] This is so despite the rapid digitization of sensitive medical records, [FN81] a marked increase in the amount of information a "medical record" now comprises, [FN82] and a number of "scare stories" about misuse of medical data. [FN83]

*1228 B. Solution 1.0: Strengthening Medical Data Privacy Rights

Understanding just what is meant by rights over intellectual property is made easier by the existence of

Title 17 in the United States and its respective siblings elsewhere. [FN84] The most politically important sticks within the bundle of rights amounting to "copyright ownership" are specifically and carefully elaborated there, [FN85] along with generally much vaguer exceptions and reservations. [FN86] They perhaps have both reflected and perpetuated cultural norms--adjusted for the political weight of various interests--about ownership of one's tangible creative output.

The status quo for privacy has been significantly murkier. The term has taken on varied meanings within and near the general "right to be let alone," [FN87] ranging from freedom from humiliating government searches and intrusions [FN88] to freedom to make personal choices free of government interference [FN89] to the ability to control facts or falsehoods linked to oneself. [FN90] Jerry Kang, in a comprehensive survey of information privacy, reviews these varied definitions and applications, honing in on a distinct meaning of information privacy that triangulates among a scatterplot of sources. [FN91] Major areas of concern include the transfer of one's personal information by another party to a third for marketing purposes, the publication of embarrassing private personal data, and the use of sensitive personal data by employers and *1229 insurance companies in making decisions that might bear heavily on one's economic well-being. [FN92]

Even if we limit our view of privacy to information privacy, however, there is simply no protection as fully developed in law as Title 17 is for copyright. The information revolution encountered a legal patchwork of information privacy rights that, by any account, is only fitfully mapped out. [FN93] There are many places where the U.S. Code defines personal information privacy rights vis-a-vis government intrusion. [FN94] The legislation that is arguably *1230 most comprehensive--the Privacy Act of 1974 [FN95]--might have become the "Title 17" of privacy had its proscriptions applied against private actors, as the report from which it drew many of its features recommended. [FN96]

There are federal laws covering the handling of highly specific and especially sensitive types of collections of personal data in private hands. [FN97] These include laws governing handling of video rental information, [FN98] cable subscriber channel preference data, [FN99] the contents of telephone calls (both *1231 landline and cellular), [FN100] credit reports, [FN101] financial transactions, [FN102] and electronic communications generally. [FN103]

At the state level, some constitutions provide generalized rights of privacy supplemented by interpretive cases, [FN104] statutes carve out particular privacy interests, [FN105] and at common law there are threads of tort that have developed for misuse of personal information since Warren and Brandeis's famous call for such actions over a century ago. [FN106]

Without weighing in on the comparative substantive importance--either to the principals involved or to society generally--of enabling control over *1232 respective types of information, a coarse comparison of the intellectual property and privacy protection regimes suggests that the former was and is more securely protected under the law.

This differential is even more striking when the transposition of parties is taken into account between the two areas. Intellectual property stakeholders have a direct economic calculus by which to measure and justify the amount of protection to insist upon, whether through private causes of action [FN107] under expanding copyright law, [FN108] enforcement of contracts that bear on control, [FN109] or funding the development and deployment of technological self-help schemes. [FN110] As noted earlier, some of the most prominent stakeholders are themselves collective organizations who can apply economies of scale in the processes of expanding and defending the reach of intellectual property rights, including the investigation and prosecution of particular infringements. [FN111]

*1233 The privacy-seeking individual is, by contrast, far less well equipped to assert her information "rights." [FN112] The Federal Trade Commission can rarely take on individual privacy violations alleged to rise to the level of unfair trade practices, focusing instead on violations that seem widespread and systematic. [FN113] For an individual to bring a lawsuit for, say, invasion of a common law right such as "misappropriation of personal data" [FN114] is simply not as easy as it is for a record company to pursue a pirate; the nature of the right makes for a less mechanical cause of action, and the aggrieved plaintiff may be fighting for dignity more than for any likely remuneration. [FN115] As for contract rights, alleged invaders of privacy may not have contractual privity with invadees, and where privity exists the "little guy" worried about privacy may be the weaker party in the contract, unable ex ante to readily negotiate, afford, or even rationally account for privacy protection that truly reflects his or her preferences, particularly when the use of personal information is ancillary to the transaction in question. [FN116] For example, few people would be in *1234 a position to dwell upon what will happen to data about their car rental as they present their drivers' licenses, sign a few forms, and pick up their keys. [FN117]

The interests that are well-organized to protect copyright are among the commercial interests who fight any movement toward strong privacy legislation, fearing that it will interfere with personalized marketing efforts. Indeed, the very music and technology industries that are building structures to defend their control over artistic data are building personal data collection and use mechanisms into those structures. [FN118] This may explain why the few existing explicit federal privacy protections are as narrow as the exceptions to copyright in the Fair Music Licensing Act; some were passed in response to specific privacy "crises," and they all faced intense lobbying to narrow their scope before passage and intense litigation to cabin their scope after passage. For example, the 1994 Driver's Privacy Protection Act was passed only in response to the stalking of Rebecca Schaefer, a well-known actress; it remains the subject of litigation. [FN119] The Video Rental Act was passed after the release of Judge Robert Bork's video rental information during his Supreme Court confirmation hearings; before passage, the measure was trimmed back to ensure that video rental stores could still sell customer lists. [FN120] The Privacy Act is credited to Watergate and, as mentioned, the private sector was exempted from its proscriptions after industry weighed in. [FN121] In essence: Rational profit-maximizing industry quite naturally works to *1235 maintain a legal framework through which it can control its own information while trafficking freely in the information of individuals. Whatever privacy's value or popularity as an abstract concept, attempts to legislate it are met with stiff resistance by groups far more organized than the individuals who covet it. [FN122]

Whatever the difficulties of using existing legal tools to solve privacy problems, privacy advocates have had little else in their arsenal to combat the loss of privacy brought on by the information revolution. Federal legislation to protect medical information has been repeatedly proposed. [FN123] To date, none has passed, [FN124] though many states have relevant statutes in place. [FN125]

Congress formally punted on the issue in 1996 when it passed the Health Insurance Portability and Accountability Act. [FN126] 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. [FN127] Some standards have already been generated through this process. [FN128] The law also set an August 1999 deadline for Congress to come up *1236 with privacy restrictions to complement the technical standards for electronic medical records. [FN129] Congress missed its deadline, and the law requires as a result that the Secretary of Health and Human Services (HHS) shall impose such standards in its stead by February 2000. [FN130] The Secretary's draft regulations were put out for public comment in

November 1999. [FN131]

The draft regulations entail substantive enhancements to privacy rights combining the fiat of rule-and-sanction regulation [FN132] with a dash of strengthened contract-like rights. [FN133] For example, health organizations may not release medical records that are easily identifiable unless certain specific exceptions apply. [FN134] Further, patients are given the right to inspect their own records. [FN135] No private right of action is contemplated for violation of any of the rule's proscriptions. [FN136] 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 the consent be revocable. [FN137]

At least one health privacy watchdog group has gone on record as being generally pleased with the regulations, noting that in several areas they protect privacy as much as the discretion granted by Congress to HHS allowed. [FN138] Still, read in light of the copyright analysis discussed above, the *1237 regulations reflect the institutional disparities guarding the respective interests at stake. A "copyright" regime of rights for privacy would entail an explicit statement of a patient's exclusive rights, with a few specific carve-outs for the purposes of "fair use," which would be quite vague and difficult for fair users to rely upon. [FN139] Instead of establishing "privacyright," however, the regulations merely subject identifiable medical data to "fair information practices"--the sort of protection identified by at least one scholar as a consistent means of undermining a solid rights regime. [FN140] These practices are standards rather than rules, requiring that the covered entities "not use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose." [FN141] Under the rubric of "scalability," the HHS draft considers implementation of these rights to be "flexible," asking each covered entity to "assess its own needs and devise and implement privacy policies appropriate to its size, its information practices, and its business requirements." [FN142] The carve- outs are, by comparison, quite explicit, allowing law enforcement, medical research, and other government interests continued access to patient records without consent, so long as certain procedural steps are followed. [FN143] HHS may ultimately exact civil penalties for violation of its privacy rules, and in some cases may refer privacy violations to the Department of Justice for criminal prosecution. However, its own proposed regulations treat both of these actions as last resorts, preferring "informal resolution" on a case-by- case basis to more formal *1238 and precedent-setting procedures that could have a deterrent effect. [FN144] As with my analysis of copyright, I do not here mean to analyze whether these carve-outs are good public policy; rather, I wish to underscore the levels of specificity and enforceability--and therefore "usability"--at which the rights and exceptions are expressed, seen in light of the political power of the interests behind each.

How much of a difference the proposed rules might make for privacy is difficult to predict, especially when one considers the backdrop of enhanced portability of electronic records that the HIPAA hastens. [FN145] As the November draft would have it, there is no private right of action for violations of regulations. Thus, ongoing enforcement by government agencies and prosecutors will be needed to guarantee respect for the new rights. Further, how genuine patients' consent will prove to be--which, once granted, permits the data free-for-all to continue--is also difficult to predict, although the regulations do prohibit conditioning the provision of medical care on consent to data sharing. [FN146]

There are other possible legal approaches to solving the medical privacy problem in the era of promiscuous publication. In one approach, Congress could enable aggrieved citizens to bring class actions representing individuals whose privacy rights have been violated, thereby discouraging misuse of medical records. Of course, with the records in custody of the defendant and the information within possibly available from other sources, those whose privacy has been violated often have no way of

knowing of the fact of the violation-- much less the source. Junk mail from a vitamin supplements company may be random or may be targeted based on records drawn from cancer sufferers. A denial of employment might be based on a bad interview or on knowledge that the applicant is HIV-positive. Furthermore, a class *1239 action regime is essentially reactive rather than preventive--at least for the current round of plaintiffs. Money damages may be better than nothing and they might help reduce future privacy violations, but the patient might well prefer that the violation never happened to begin with. Finally, potential industry defendants would likely bitterly oppose such a system because it introduces an element of uncertainty into their choices of what to do with the medical information they ward.

A second approach could be to create a general privacy right with respect to medical records along with a safe harbor provision for those who wish to use medical data. A safe harbor provision generally sets up a set of standards with which an entity can comply in order to ensure freedom from legal liability. It functions as an incentive to behave responsibly. [FN147] Use of safe harbors in the information privacy context has recently become an issue in the United States in response to the European Union's directive on information privacy. [FN148] Since the EU began requiring certain privacyguarantees for participation in information exchange, the United States government has been working to negotiate a safe harbor provision that would help U.S. entities both know what they needed to do to comply as well as avoid liability. [FN149] *1240 Certain privacy advocates have lauded this approach. [FN150] This is a promising approach, but still requires an enforcement mechanism that might fall short.

The elephants of the music industry found it easy to bend law to their interests, but still found it unfulfilling because law is a difficult tool to employ against the individual gnats that would flout it. Privacy advocates may face roughly the inverse problem: They will find law more difficult to bend to their interests, since they face more organized and powerful opposition to the creation of clear, substantive rights. Moreover, while the elephants who wish to consume and share data in the medical privacy context may be more responsive to the prod of legal enforcement than their individual counterpart consumers in copyright, it may be harder for the individuals who are sources of medical data to engage the corresponding mechanisms of enforcement. Even the HHS regulations--drafted by policymakers quite sympathetic to privacy interests-- couple formal enforcement teeth with paeans to "flexibility" for those charged with guarding privacy and a desire for "informal resolution" above rule and sanction.

C. Solution 2.0: Technological Self-Help Through Trusted Systems

A patient's record and a musician's record may appear quite different to the casual observer, but as we have seen, both boil down to data susceptible to an Era of Promiscuous Publication, [FN151] harming the interests of their respective owners.

As the music industry is discovering--enough so that its former horror over the Internet is giving way to an embrace--we can seek to protect against technology's perceived excesses by having the desired limits themselves be of technological character, embedded in the very scheme thought to be causing the potential for abuse.

Consider three of the interrelated new rights proposed in the HHS draft regulations: a patient's right to inspect his or her information in a medical database, a patient's right to give consent before that information is transferred for many purposes, and a patient's right to receive an accounting of instances in which information has been disclosed. [FN152]

As we have seen, while the original Act's administrative simplification provisions are intended to bring about easier information sharing among *1241 holders of medical data through quite thoroughly elaborated technical standards--which makes an invasion of privacy easier [FN153]--the accompanying privacy rights implementations float at a much higher level of abstraction, variable from one entity to the next in the name of "flexibility."

For example, a hospital with a highly efficient electronic records scheme could nonetheless insist on fulfilling the patient's right to inspect data or gain an accounting of its redistribution by requiring the filling out of a paper form, performing a less-than-instantaneous manual search, and then releasing photocopied sheets in fulfillment of the request. [FN154] Indeed, this is just how the "Medical Information Bureau" clearinghouse--a Massachusetts company that gathers and redistributes health data on fifteen million Americans for insurance assessment purposes--currently allows patients to review the records accumulated on them. [FN155] After the request is fulfilled, a new cycle of paperwork would presumably be necessary to see updates to one's data.

Similarly, consent for redistribution of data might be obtained through a stylized exchange of paper at the initiation of the relationship between a patient and an entity covered by the regulations. While the regulations insist upon a thorough disclosure to a patient of the intended uses of information being collected or generated, including an explicit statement of intention to *1242 sell or barter the information, [FN156] it appears that a blanket authorization can be obtained once and never revisited unless the patient seeks to do so, presumably through another flurry of paperwork. While this may not satisfy privacy advocates, [FN157] any stronger rendering of consent--for example, requiring assent for each nonmedically necessary release of identifiable patient data--raises transaction costs on the releaser that do not satisfy others. [FN158]

Finally, whatever the legal rules about privacy, an untrusted (in the technical sense) implementation of whatever information-sharing standards emerge from the Act could enable widespread information piracy of just the sort that even the music industry--with all its sophistication, statutory rights backing, and political power--feared in the absence of technical protection schemes. It is simply too easy for someone near a health information system to be able to abuse its contents, even if she is not free to do so. This may be clearer if we again frame the current Act and corresponding privacy regulations through the lens of copyright enforcement: It is as if Congress had actively promoted--nay, mandated--the development and use of the highly efficient and non-rights-architectured MP3 compression standards for digital music, leaving the formulation of protection from any abuse to a government agency which would prescribe general regulations lacking any private right of action.

*1243 Now imagine for a moment the patient control possible for these same three rights in a world where privacy advocates have succeeded in creating a trusted system that provides the patient with as much lopsided control over her medical records as the music industry's privication architecture seeks to provide for its intellectual property. Built on an ability to discriminate on the basis of consumer characteristics and on the provision of desired information to consumers with different kinds of interests in the data, the architecture could effect control not readily possible--not even administratively so--without it.

Suppose a patient could "log in" at any time to the databank of her one-stop HMO. [FN159] She could do so through her own personal computer over a secure connection on the Internet, or through a terminal provided for this purpose at a library or health care provider. With a few mouse clicks she could view her own records as readily as a physician seeking access to them through similar computer-

mediated means. She could view an audit log revealing who has seen her records and when, perhaps setting permissions as to who among various categories of potential viewers--or even who among specific people--is authorized to look at which pieces of information. She might, for example, want to exclude her notes from psychotherapy from easy access by anyone but her therapist, even if her therapist and primary care physician are employed by the same institution. She might want to allow those to whom she gives permission a chance to see the data but not save it--so an outside physician could look at her records but not print them or save a copy into another databank. The emergency room attending physician may be able to view an incoming patient's records for the duration of her visit to the emergency room, and lose access thereafter. This makes it possible for the record holder meaningfully to change her mind about certain disclosures to which she had previously agreed: She might allow baby products companies to know that she was recently in the clinic for an ultrasound related to a pregnancy so that they could identify her for the purposes of sending her coupons, but then revoke permission to include her name on targeted mailing lists should something go wrong with the pregnancy. [FN160] She might choose to *1244 allow a local pharmacy to view a list of her recent prescriptions at no charge for the purpose of offering her a better pricing package, while charging an over-the-counter drug company $100 to see a record of her vaccinations, prepaid. She might even ask that her spouse be permitted to make such rights determinations in her absence, or insist that in no case will her rights be more expansive than the list recommended (and electronically made available) by a privacy watchdog group. [FN161]

Indeed, she might agree to the use of her medical data for marketing purposes only so long as there is a division between those who conceive of a promotional mailing (and know its criteria) and those who actually view the mailing labels and affix them to the promotional materials for mailing. [FN162] An extreme implementation of the system would even allow the patient simply to delete her records, or extract them from the system and keep them in her personal custody. [FN163]

While this hypothetical might seem appealing to some privacy advocates, it represents a balancing of interests that ignores most interests of the consumers of medical data--politically implausible at least, and perhaps even simply bad policy. It permits the possibility that Scott McNealy could frighten a wave of patients into deleting all their medical data en masse, [FN164] or that a particularly compelling telemarketer could flim flam patients into accessing and retransmitting all their sensitive medical information. [FN165] However, *1245 no matter how unappealing, these potentialities attest to the true range of power of trusted systems architectures.

I do not seek here to build a case for one or another particular allocation of rights and constraints with regard to medical records. Rather, I wish to emphasize that a well-designed trusted system of rights to medical data could be both powerful and flexible.

The actual policy choices underlying what rights architecture to build--what powers to grant to the patient and what exceptions to insist upon in a trusted system containing her data--are as difficult as any other policy choices involving rights (or property) allocation. The process by which HHS would determine how much "trust" to include in its interoperable standards, and whom to assign each of the sticks within a bundle of constraints, would itself be political. Privacy advocates would have to strategize to focus on just which elements of medical privacy were most important, and which could be left open within a negotiation at which other interests--medical research, government, direct marketing--are also well represented at the table.

Indeed, to the extent that privacy is simply a dignity interest, rather than a more readily calculable remunerative interest like protection of copyright, it is all the harder for those who embrace it properly

to calibrate pressure to vindicate the interest to its perceived degree of importance, whether arguing for overall legal protection or weighing whether to pursue an individual action. Thus, if government is stepping in to subsidize and ultimately mandate a system for interoperable medical records, one may wonder why it should be any easier for patients to see their preferences reflected in that system as "trust" when their privacy has not been incorporated into traditional federal privacy frameworks to begin with. Isn't the public choice problem the same whether one is trying to convince Congress to mandate strong privacy rights as legal rules or within software code? I reflect on this issue in Part V and argue that code helps break the logjam.

IV. Beyond the Publisher: Privication to Satisfy Both Producers and Consumers of Data

Privacy advocates will only be able to benefit from the power and flexibility of a well-designed trusted system if it is politically and economically *1246 possible to implement one. A trusted system to protect music is emerging from market actors; apparently a handful of record companies--and technology companies--can overcome a collective action problem and invest in an interoperable protection scheme of benefit to all. There is no such phenomenon yet taking place for medical records; the collective action problem among millions of patients may make market-based development of a comprehensive medical trusted system quite difficult, just as it has been difficult for the market actors of hospitals, HMOs, and insurance companies to generate even an untrusted interoperable medical records system clearly of benefit to all.

Rather than being able to generate protection themselves, then, those who wish to protect medical privacy will be nearly as dependent on government intervention as they would be if they sought a legal rights-based solution. Yet their energy may still be better spent on the creation of a trusted system for medical records than on a new rule-and-sanction regime, because it will benefit them more than law and, done well, threaten competing interests less. The analysis of privication architectures in Part III suggests that it may yet be politically feasible, even desirable, for all those with a stake in rights to medical records--privacy advocates, medical researchers, and doctors alike-- to create a trusted system that seeks to embed rights satisfactory to most interests.

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 then 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.

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 having ultimately to resolve matters in a coarse way as "owner" and "nonowner." A patient might wish to have the right to delete 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, and no longer being available for marketing purposes, while still being included in scans of records by medical *1247 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, and among the purposes for which the access is sought. 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 her record except that which is explicitly marked to be held back by an authorized doctor. Then, at least, she would have a sense of what she did not know and why, and her access to some parts of her record would not be held hostage to other parts deemed, for some important reason, off limits even to her. All this could be done with a minimum of administrative burden on the database custodians.

The granularity of rights available within trusted systems also suggests that we need not choose between creating horizontally integrated records (all records across a given institution) and vertically integrated ones (all records pertaining to a given individual, wherever those records may be). Granting a patient seamless access to her records among all covered institutions means that getting a second opinion from an outside doctor--or transferring to another health care provider entirely--can be accomplished without barriers of paperwork and delay endemic to patient access to current automated systems such as the MIB. [FN166] This can promote competition without depriving institutions of the horizontal access to records deemed necessary for utilization review or other purposes.

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. The system might even be constructed to allow patients to set preferences for access to some of their personal data, but discourage the creation of a market by denying them the ability to sell other data. Patients could thus be restricted from handing over highly sensitive information for a pittance without realizing the implications of the transfer, while still being able to control the information. 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, already recorded in *1248 many instances, to help design a healthy diet or correlate diet with a given disorder--an ability to efficiently set sophisticated gates around data elements could be critical. At the very least, a granular trusted system allows for those on the margins who care dearly about personal privacy to limit circulation of records, without requiring a similar default policy that binds all other patients.

Third, privacy advocates may learn from the music industry's structure rather than its technology: The use of aggregation of preferences may be applied to the problem of ill-informed (or simply disinterested) patients being asked to specify a battery of preferences about the disposition of their sensitive medical data. ASCAP and RIAA are instruments of aggregation of preferences; to clear rights to a covered song, one consults with ASCAP without having to reach the original author or performer. One could imagine an initial form presented to an incoming patient with some notice of the availability of a system through which to view records and exercise certain rights with respect to them. The form could ask a few coarse, basic questions, the answers to which would help fill in the initial patient-set constraints of the elaborated trusted system; it could also offer descriptions of three or four organizations whose preferences the patient could initially adopt as her own. Thus one could check a

box, say, for the American Medical Association, the Electronic Privacy Information Center, or the AARP--importing preferences in one step that could be revisited at the patient's leisure later. [FN167]

Finally, trusted systems' Newtonian inertia of rights enforcement will help 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. [FN168] Indeed, Congress might *1249 find it politically more difficult to undermine a privacy regime--to affirmatively strip privacy rights accorded by HHS--than to simply fail to pass legislation establishing the rights in the first instance. The physics of trusted systems are thus well suited to a Congress that only rarely allows a bite of privacy's legislative apple.

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.

Conclusion

No practical combination of law and technology will be a panacea for the deep problem of control over information. Pinpointing the rights to be protected and the exceptions to apply is an ongoing exercise in civic discourse. The ability to elaborate those rights in detailed, self-executing ways could remove some "give" in a system that also counts on norm and dynamic interpretation-- respect for law, and for its substantive aims by those subject to it, and respect for the distinct circumstances of each case by courts enforcing it--to arrive at a just status quo. [FN169] In the case of privacy, only some of the matters of currently pressing concern--for example, the routine use of personal information for marketing, employment, or insurance purposes--are satisfied by a trusted privication regime. Embarrassing personal details can be publicized as soon as an indiscreet (if authorized) viewer of personal data chooses to gossip, no matter how difficult it is for the viewer to print the data or regain access to it later. However, despite its shortcomings, a trusted privication architecture for medical data offers a kind and degree of protection that law alone cannot easily emulate.

The Era of Promiscuous Publication is upon us, and for publishers of intellectual property the quite different Era of Trusted Privication is about to enter on its heels. A rare and fleeting chance for the latter era to come about for medical privacy in the United States is now within grasp. A system is already under construction specifically to leverage the fruits of the information age--quick processors, immense data storage, ubiquitous networks-- into a drastic lowering of the costs of sharing personal medical data. The question is how much trust it will have--and who will be thought of as its "customers." [FN170] The government has already taken on the ambitious task of *1250 shaping a comprehensive set of standards for medical records interchange, [FN171] and private efforts are also under way to develop such systems. [FN172]

If the moment is not grasped now to develop and standardize privication architectures, the untrusted system for medical records now under development will have a momentum all its own. As the power of technology is harnessed to move us from a Gutenberg status quo of personal information sharing toward a more promiscuous one, we must consider means to impose agreed-upon limits that are grounded in that technology.

Stanford Law Review
May, 2000

Comment

*1585 TRUSTED SYSTEMS AND MEDICAL RECORDS: LOWERING EXPECTATIONS

Henry T. Greely [FNa1]

Our world--perhaps especially our academic world--is intensely specialized. Expertise in privacy and the Internet would seem readily transferable to issues of the privacy of electronic medical records, but there is a very real gap. Jonathan Zittrain has taken his knowledge of the possible uses of "trusted systems" in the electronic delivery and control of music and applied it to electronic medical records, a field with many experts and a voluminous literature, [FN1] which Zittrain, quite understandably, has not mastered. (Neither have I.) These forays across the growing number of deep disciplinary and subdisciplinary chasms are dangerous. Specialists may well dismiss the interloper with a curt "he doesn't know the territory." But the risk must be taken. Unless we can compare similar problems in different settings, our ability to learn, and to improve, is crippled. Given the falling odds that even one person will be expert in both fields, efforts like Zittrain's need to be encouraged, not trashed.

But, in fact, Zittrain doesn't know this territory. The issues that are important for the privacy of electronic medical records are quite different from *1586 those that affect the use of trusted systems in music distribution. Each is just another collection of ones and zeros to a computer, but their cultural significance, and uses, are critically different. Zittrain admits that trusted systems would not be a panacea for the problems of medical records privacy, but argues they may be useful. I agree that they may have some uses, but I am considerably less optimistic about their value in this context. This commentary briefly explains my reasons.

Two key problems limit the application of trusted systems in the medical context. First, trusted systems do not speak to the crucial questions. Music companies want to use trusted system to distribute the ones and zeros of their product to people while limiting subsequent uses--mainly copying and distribution. Their problem is how to control subsequent uses by those who first receive the product. As to the initial recipient, only one question is very important--has he paid for the music? Third parties do not have important roles in this private entertainment transaction.

Patients, the "trustors" in Zittrain's vision of electronic medical records, want to use those systems to make sure that their information is available to many potential users. The identities of the relevant users cannot be specified in advance, nor can the patient count on being physically or mentally able to authorize their access when most needed. In addition, many third parties will have either compelling or powerful claims to access to those medical records. And patients will be far less able to insist on the full strength of their trusted systems than either music companies or music consumers. Thus, with medical records, the crucial question is not how to control secondary access but who should get primary access. The answers to that substantive question may greatly reduce the protective power of trusted systems. I will expand on this point at length below.

But, first, consider another key difference between digitally recorded music and digital medical records. The music company sends a product that is only valuable if it can be used in a digital format,

with all its ones and zeros, to reproduce the music. [FN2] For the distributor's interests to be substantially harmed, the whole file (or a large portion of it) has to be transferred to another digital apparatus. The electronic medical record, though encoded in ones and zeros, is largely words (with a few pictures). The patient's interests might be harmed by a very small part of that file--for example, the words "acute depression" or "HIV positive" or "elective abortion." And that harm *1587 can take place when those words are transferred, not just to another computer or other digital instrument, but to a printout, a photograph, a piece of scratch paper--or a human brain. This second difference makes controlling the subsequent uses much, much more difficult.

Now, let's look at the substantive question of who should have access to a patient's medical records. Consider issues of access to patient medical records by medical providers, health care payers (including employers), medical researchers, marketing users, and the patients themselves.

Interstate 80 runs from the Manhattan end of the George Washington bridge to the San Francisco end of the Oakland-Bay Bridge. A driver might have an accident on any of the intervening 3,000 miles and need emergency medical care. That care might well be improved by access to the patient's medical records. Will emergency room physicians be able to see them? Assume the accident results in a long hospitalization. Who in the hospital might need access to the patients' records? All doctors who might be on duty during the hospitalization. All the nurses. The hospital pharmacy. The surgeons, anesthesiologists, and intensive care specialists. The resident on duty when the patient codes. [FN3] Almost any professional in the hospital could have a valid need for that information, at any hour, whether or not the patient is able or willing to give her permission to see it.

One could imagine a trusted system that permitted a patient to choose which health care providers would have access to her data, but would the overall framework allow a patient to prevent providers who need the medical records to care for the patient from getting access? Hospitals, and their politically powerful trade associations, will not be eager to accept that. And, if patients were allowed to impose such limitations, how many patients would be likely to resist the hospital's argument for a "voluntary" expansion of access--to their local hospital staff, to emergency rooms, to the staff of any hospital where they are admitted. Any such expansion, however, would give the, quite literally, millions of health care providers in the United States the power to access records, at least under some conditions. Any one of those people could breach confidentiality and publicize the medical records of a famous patient, an acquaintance, or anyone else. The medical advantages--to patients--of the more widely accessible electronic records make it unlikely that trusted systems will be applied strongly enough to avoid the resulting risks to privacy.

Those who pay for health coverage also have a legitimate interest in access to medical records. At the most basic level, they need to know how much to pay to whom. The desire to simplify billing was a substantial driving *1588 force in the federal legislation that both encouraged electronic medical records and required Congress or the Department of Health and Human Services to protect their confidentiality. [FN4]

But payers also have compelling interests in reviewing medical records to make sure that their funds are spent honestly and wisely. Utilization review is common in American medicine, in health maintenance organizations and in health care systems not usually viewed as being managed, such as Medicare and Medicaid. [FN5] Many institutions have legitimate interests in overseeing how care is delivered--HMOs, insurers, government programs, capitated physician groups, hospitals, and, most worryingly, employers. Employers are interested because they pay for health care for about 150 million Americans. If they purchase coverage from insurers or HMOs, their employees' utilization of care

almost always affects the rates they pay. For a variety of legal and economic reasons, most large employers self-insure. As the insurer, the employer pays the bills and manages the care--or contracts with someone else, often a health insurance company, to do so. If a self-insuring employer wants to make guarantee that its employees and their dependents with HIV are receive proper medical treatment, the employer needs access to their medical records. But, of course, ensuring that the knowledge the employer gains from those records will be used only for such review is a very difficult problem.

Medical researchers perform important functions for which they need access to patient medical records. Vital questions, from genetic associations of disease to the most cost-effective (or highest quality) way to provide maternity services, require that kind of data. Some of the research will have clear commercial ends, other research will have clearly non-commercial goals. For much of the research, the existence of commercial implications may not be known for years. Medical researchers not only want that data, but, to a large extent, already have it. Patient records from Medicare are widely available on massive data tapes. Although the routine use of patient data, in Medicare records and elsewhere, usually requires that the data not be "individually identifiable," this, as noted below, is a poor protection. A new approach, which required patients' consent, possibly through a trusted system, before researchers could use their medical records, might improve the *1589 status quo. [FN6] But the substantive decision whether to require such consent is the hard, and fundamental, question--not whether such a consent requirement should be implemented through a trusted system.

Even marketing uses can be--or can be made to seem--more appropriate in a medical context. The patient's health plan might, for example, want to make patient information available to a firm that markets a health-related service not directly provided by the plan. A plan might pay for durable medical equipment, such as wheelchairs, but offer consumers a choice among brands. In that context, its provision of data to the wheelchair firms about the names, addresses, and needs of plan members may be useful. Requiring patient consent to that specific disclosure may be overly expensive--and, for the patients, overly annoying. Even if the health plan does not pay for the service, one may argue that its help in getting information to consumers about their health needs is legitimate. There would seem to be little reason for concern if a health plan that provides, for an extra fee, its own smoking cessation program advertises it to its members who smoke. Does the balance change that dramatically if the plan does not handle smoking cessation internally but, instead, encourages its members to use particular firms by letting those firms know which members to contact?

Finally, allowing even the patient direct and easy access to her own medical records may cause problems. Currently, in most states, patients have statutory rights to review and get copies of their medical records without having to seek them in discovery as part of litigation. [FN7] But, when paper records are involved, the process is time consuming and can be expensive. Increasing the ease of the patient's access to information should lead more patients to review their records. What could be wrong with that?

Well, although the notes doctors put in patients' charts will sometimes be inaccurate, they will more often be accurate but not flattering to the patient. If the physicians know that patients could easily and quickly get access to those notes, the notes might be less candid and less accurate. The failure of a doctor to note her suspicions of a patient's alcoholism in the medical record could later have dramatic, even fatal, consequences for the patient at the hands of another doctor. Similarly, giving a patient a "right" to "correct" medical records can raise problems. Accepting the patient's word that the record is wrong could also lead to misleading medical records and potentially bad health consequences. Access to the records would have to be only the *1590 first step in a process, sometimes complicated and

contested, of "correcting" them. And, of course, any time consumers have access to data only by using passwords or some other protective device, the risk that the protective mechanism will be forgotten, lost, stolen, or otherwise abused is substantial. These problems do not mean that patients should not have access to their records or the power to begin a process to correct them. To the extent we decide to allow such rights, a trusted system may well make sense for implementing them. But that question of extent is the crucial one and it is not made much easier by the use of trusted systems.

In each of these circumstances, public policy reasons of some real importance may prevent patients from exercising the full powers that trusted systems could give them. The interests involved in downloading music seem almost trivial by comparison. The music companies want to get paid for their product; consumers want to be able to make copies freely. Few, if any, other parties have legitimate interests in the data/music. Life in health care is much, much more complicated. Two additional complications deserve mention: the use of information that is not "individually identifiable" and the possibility of patient waivers of trusted system protections.

Currently, regulations, such as those proposed by HHS and the "Common Rule" governing most human subjects research, often distinguish between individually identifiable data and data that is not so identified. Thus researchers can get relatively easy access to information about medical care paid for by Medicare as long as the records have had personal identifiers stripped from them. This distinction is meaningless in music--making the data stream that is the music anonymous as to either the performers or the producing firm would not affect the need to limit subsequent use. But in medical records the distinction is often legally important.

The problem is that, although legally important, the process of transforming medical records into data that is not "individually identifiable" is increasingly meaningless for protection of patient privacy in medical records. The amount and detail of information in a medical record, particularly if it is a patient's comprehensive electronic medical record, integrating records from different health care providers, is so rich that, with a little effort, the patient could often be identified. Consider three data points only--date of birth, place of birth, and sex. For many people, especially those born in small towns, that data, combined with publicly accessible birth records, will identify them. Or consider a white male, born in Arkansas in August 1946, married with one daughter, currently living in the 20500 zip code in Washington, D.C., [FN8] whose chart reveals he had knee surgery in the last few years. No prize for guessing that identity. The crucial question here is whether individually *1591 identifiable information will be more broadly free from the patient's control, as exercised through a trusted system. Again, the use of a trusted system does not help with the hard problem.

There is a last important distinction between the music industry and health records. For the consumer, the purchase of music is discretionary. Even the most music--besotted fan really can live without it. The sale of music, in general, isn't (very) discretionary for the music company, but any individual sale is not very important--and it has lawyers and employees considering the general constraints it should impose. Health coverage of some sort (although, shamefully, not universal in the United States) is a necessity--at least for anyone who needs medical care. Patients, if they can, will have health coverage--through Medicare for 40 million Americans, through Medicaid for 30 million, and through employers for about 150 million. Only rarely will an American purchase her own health insurance; often she will have no choice about the coverage provided. And, of course, the patient will have little sophistication about, or understanding of, the proposed waivers for transfer for medical, payment, research, or other uses.

Now, assume, implausibly, that electronic medical records end up covered by trusted systems with real

teeth--no disclosure, to anyone, for any purpose, without express patient authorization. But further assume the legislation allows health care providers, insurers, researchers, and others to ask for some general advance waivers. It seems to me unlikely that such consumers, in the acquisition of such a vital product, will, in any large numbers, take control over their own health privacy or even, as Zittrain suggests, give that control over to an intermediary. In practice, as Zittrain concedes, the trusted system method might only allow a few patients with particularly strong views of privacy to opt out of some disclosures. (As noted above, there are strong arguments against allowing even these patients to opt out of all disclosures.) How highly should society value the protection of that minority interest?

I have to make one final, different, but important point. Making analogies between existing practices across industries, or cultures, is extremely difficult--but the music distribution system does not use trusted systems. Yet. Zittrain paints a powerful picture of why such systems should exist and should work well, but, "it's always hard to predict things, especially the future." [FN9] The music industry and the computer industry, Zittrain reports, are *1592 cooperating and moving toward implementation of trusted systems. Will they reach agreement? Will they be able to make the trusted systems work? What will be those systems' unanticipated costs--and benefits? We cannot, by definition, know the unanticipated problems; we can only predict, with confidence, that some will exist. At this point, there is no functioning large-scale trusted system model to emulate--there is just a vision to ponder.

But medical records, on the other hand, do exist and they are rapidly become more electronic. The timing issue implied by the different status of music industry trusted systems and electronic medical records is particularly salient here. The pattern for electronic medical record privacy may be laid down before this commentary is printed, let alone before we have experience with trusted system in music distribution. As Zittrain notes, the Department of Health and Human Services, following orders from Congress, published a notice of proposed rulemaking on electronic medical records last November. It remains unclear whether that rulemaking will go forward; if it does, it may well be an interim step, neither adopting nor precluding a trusted system model. But it is also possible that this year's decisions will affect the future shape of medical records privacy. It is implausible that those regulations will be built on an untried model of trusted systems. At best, one might hope that the regulations be drafted with an eye to keeping open the possibility of using trusted systems. Even that may be more than this important and intensely followed initiative can deliver.

In this article Zittrain has performed the valuable task of trying to transfer experience--or, in this case, anticipated experience--from one field to another. This effort is often useful, but always risky. Zittrain's article on trusted systems does contain useful ideas. Giving patients some access and some control over their records may be important. In some respects, the audit trail, the patient's access to the audit trail, and the potential deterrent effect of that access, may be the most valuable part of the systems. That the biggest issues in medical privacy are unlikely to be affected by such systems does not mean they will worthless in the medical context. It does mean that, even if trusted systems do prove effective for distributing music systems, they will not be "the" solution to the problem of medical records privacy. Zittrain has convinced me, and I hope others, that they are worth watching to see whether they might play a useful role in implementing whatever solutions *1593 we choose to the hard problems of protecting the privacy of electronic medical records.

Stanford Law Review
May, 2000

Comment

*1595 PRIVICATING PRIVACY: REFLECTIONS ON HENRY GREELY'S COMMENTARY

Jonathan Zittrain [FNa1]

My article in this issue of the Review [FN1] makes the claim that an appreciation of the power of "trusted" or "privication" architectures could help break political and conceptual logjams suffered within long-running debates over privacy. Trusted architectures include systems of hardware and software that take note of various entitlements to the data they store--and automatically enforce those entitlements. I use "privication" to describe a structure of self-enforcing entitlements that provides access to data to a large audience as traditional publication does, while narrowing the scope of access in a way that precludes easy wholesale copying and retransmission of the data. The information thus retains private (and privately-controlled) qualities.

Prof. Greely's commentary evinces a healthy skepticism about the applicability of these architectures to the problems of medical data privacy. He makes several points; I reflect on each below.

Greely's first worry is that even a small portion of a record passed by word of mouth can cause harm or embarrassment. This is surely true, and while trusted systems can help by offering audit trails that may clearly define who would have been in a position to breach confidentiality, my concern is less with the occasional damage that gossip can wreak on privacy than with the wholesale abuse made possible by the internetworking of medical data. A comprehensive interoperable medical database will entail a sea change in the ability to search for damaging information on an individual, and to put millions of records to uses never before possible, from telemarketing to employment screening. Trusted architectures can be central components to a firewall that, together with traditional legal protections, can best advance the benefits of the information age while minimizing its intrusions.

*1596 Second, Greely finds much of the work on trusted systems to be conjectural. The problem, however, is that the technological forces at work here may have only two phases: too early to tell their impact, and too late to do anything about it. It is technically trivial to integrate a notion of patients' rights into the coming medical database while it is still on the government's drawing board, but it will be quite difficult to change the standards once they are deployed. I do not urge that we forsake a legal framework for a technical one; rather, I want our values to be reflected in and reinforced by each. In an area as sensitive as privacy, we have a responsibility to act while much of the genie is still in the bottle; we should treat our personal health data as if it were as least as precious as the music industry's latest chart-toppers.

Third, Greely points out that trusted systems cannot help answer the hard normative questions of medical privacy. If he means just how to assign entitlements--for example, how much access medical researchers should have to individually identifiable information, or whether patients ought to be able to view their entire records--this is true. The normative questions are enduringly difficult, and trusted systems are not elixirs to simply make them go away.

Instead, I look to trusted architectures as one means of empowering those who routinely traverse the privacy territory to come to creative, meaningful agreement--this includes experts like Greely, along with advocates for producers and consumers of personal medical data, whether patients, doctors, hospitals, researchers, or businesspeople. How can trusted architectures empower those at the negotiating table?

First, they allow for "baby-splitting" to take place: Conflicting interests that had previously seemed zero-sum can be more readily reconciled thanks to the nuanced ways in which a privication framework can enable access to data. For example, a patient may wish for any doctor performing emergency treatment upon her to be able to view her primary medical records at the touch of a button--while not being able to see her psychotherapist's narratives. Trusted architectures can readily unbundle some aspects of patient data from others, and they can make "access" to data mean less than full custody of it. Just as music publishers may wish to let fans hear songs a limited number of times without being able to easily copy or share them, many privacy concerns can be ameliorated by allowing access medical data for some purposes without that access entailing possession of the data forever.

Second, trusted architectures can help substantive decisions about entitlements stick. Again, these substantive decisions are not easy to make, but we are in the process of digitizing and networking our health records--some decisions will have to be made, if only by default, even as the debate continues. After Congress found itself incapable of meeting its own deadline to legislate privacy standards, the U.S. Department of Health and Human Services has attempted to do so. HHS's standards include some notions of patient *1597 rights, but these rights may end up only hortatory in practice. Individuals are not in a good position to monitor the custody and use of their records in "untrusted" databases, and HHS concedes that it has little infrastructure to support enforcement of the privacy standards it has devised, nor authority to regulate the use of health information by parties outside the immediate circle of health care providers. [FN2]

Thus, while Greely may not believe that controlling redistribution and use of medical records is really the issue once the hard normative problems of primary access have been solved, there is good reason to be concerned about both. HHS states the problem well; it falls short only in recognizing the full range of tools available to it for solutions. It is already working on standards for the digital representation of health care information; augmenting those standards with a trusted architecture that limits secondary uses both speaks to the problem and is squarely within HHS's authority. This can prevent privacy violations before they occur--something that should be as heartening to lawsuit-weary corporate custodians as it is to individual record-holders.

Indeed, while there are plenty of differences--the foremost cultural-- between the ones and zeroes that make up digital music and those that make up personal medical data, both are now irrevocably headed to a networked environment. Trusted systems are a concrete way to think about the tough, if subtle, gates that will channel our data from one person to the next. To underestimate the power of these gates as we build our network--to eschew their common use within a broader legal framework--is to miss an opportunity that will not knock again soon. The true dimensions of a privication framework are being worked out by publishers at Internet speed. They leave important lessons for those who care about privacy in their wake.