Introduction

Keeping Secrets

Dale Carpenter†

The right to privacy is the power to keep secrets. It is a power conferred in one form or another by the Constitution, by statute, and by tort law. It hinders the ability of the government and other citizens to know things about us that we -- often for very good reasons—would rather not have them know. It is a power that acts as a counterweight to the power of the state and of other citizens to monitor–often for very good reasons–what we do, what we read, what we say, and with whom we associate.

Given the right to do so, most people would probably keep private as much information as possible about themselves. At the same time, we would like to be able to know as much as possible about everyone else. Much of that information about others has some value to us, aside from satisfying a taste for gossip: Lenders want accurate credit information, sexual partners want to know about sexually-transmitted diseases, and the police would like to know who is growing marijuana in an in-home garden.

We can, of course, make it a crime to lie on a credit application, to expose others to the risk of disease, and to grow pot. But deterrence of these activities will be imperfect, providing cold comfort to, say, the mortgage company that has lost a small fortune it is unlikely to recoup as a consequence of a bad loan. Or consider a more searing example of the failure of substantive criminal law alone to prevent harm. It is a crime to crash a plane into a skyscraper, but that does not prevent it from happening. How much better it would be to know in advance the hijackers' plans. But that would require monitoring them and the often innocent people associating with them. For every such investigation that uncovers and thwarts an attack,

† Associate Professor, University of Minnesota Law School.

there will surely be many that discover nothing more than that Mohammed is cheating on his wife. Access to advance information about others adds a layer of protection mere criminal prohibition does not provide, but that is a benefit with an attendant cost.

A government moved only by a concern for order would have little reason to limit its own power to snoop on its subjects. It would reserve for itself the full power to access citizens' financial records, medical data, regular and electronic mail, library and video rental records, book purchases, and so on. While the state could not, under present technical constraints, amass and analyze all of this information in a useful way all of the time, it could surely alter citizens' behavior simply by possessing the publicly-acknowledged power to inquire as it pleased.

Yet, quite aside from the constitutional constraints they face on such surveillance and inquiry, the federal and state governments *have* limited their own powers to pry into citizens' lives. Why? Because, it turns out, they must answer democratically to a polity concerned about more than order. There is a constituency for privacy consisting of almost the whole of the American people. Even as Americans demand safety and security from government, they deeply distrust it. So anytime more powers are proposed for law enforcement authorities or for administrative agencies, organized lobbies sound the alarm of repression. That is a brute cultural fact evidencing a powerful national consensus.

It has become a commonplace to say that September 11 changed everything. What the writer or speaker usually means by this is that Americans have re-calibrated their views on the relative importance of individual civil liberties and the common good. Now, it is said, people are far more willing than before September 11 to accept restrictions on their personal liberties in the interests of public order and national security. These restrictions may take the form of increased prosecutorial powers for federal and state authorities, greater scrutiny of individuals' associational ties to groups supporting Arab or Islamic causes in the Middle East, racial profiling of people who look Middle Eastern, more thorough searches of our persons at airports, and more state surveillance generally over our lives. Polls taken immediately after the horror of September 11

seemed to confirm the shift. The USA PATRIOT Act,[1] passed with little debate or dissent just weeks after the attacks on the Pentagon and the World Trade Center, legislated it.

I suspect this commonplace observation overstates the effect of September 11. The opinion polls upon which it relies are a snapshot of a fevered moment; they are not etched in marble. The Attorney General did not get everything he wanted in the PATRIOT Act. And the parts of the PATRIOT Act that many regard as most objectionable on civil liberties grounds will in time expire of their own force. As time distances us from that awful day, and unless there is another such domestic shock, public opinion may well shift again. Like many other national traumas, September 11 may in historical hindsight be seen as a jolt that perhaps necessarily–but at any rate, temporarily–induced a retrenchment on rights.

But if the September-11-changed-everything idea overstates the significance of the event, it also understates the extent to which, at least in the area of privacy, some recalibration of the balance between liberty and order had already begun quietly to take place. This symposium issue of the *Minnesota Law Review* is dedicated to examining the degree to which that shift had begun, the costs and benefits of the new legal rules affecting privacy, and the advisability of further changes. The symposium focuses on three areas: financial data, the Fourth Amendment, and medical data.

Not one author in these pages takes up the cause of either total government surveillance, on the one hand, or complete individual privacy, on the other. But, as readers will learn, eschewing those extremes leaves a lot of room for disagreement. One large area of disagreement in this symposium, cutting across the three issue areas, centers on the question whether the judicial function in assessing privacy claims should be to identify a substantive value protected categorically from intrusion or whether it should be to engage in a straightforward balancing of the costs and benefits of protecting privacy versus the common interest in obtaining information.

Professor Marc Rotenberg's foreword[2] begins the issue by noting that we might usefully think of "privacy" as encompass-

1. Uniting And Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 15 Stat. 272 (2001).

2. Marc Rotenberg, Foreword, *Privacy and Secrecy After Septemter 11*, 86 MINN. L. REV. 1115 (2002).

ing demands for withholding information that come from two distinct parties. There is the demand of individuals for privacy from the government, which is the focus of most of this symposium's attention. But there is also the government's own desire for privacy (or as Rotenberg puts it, secrecy) from the public.[3] As individual privacy contracts, government secrecy expands.

Rotenberg's piece shows how the move toward more state power–here in the form of the state shielding its own actions from public view–began before September 11 but has accelerated in its aftermath. This includes greater prosecutorial powers under the Foreign Intelligence Surveillance Act and a more lenient standard for preventing disclosures of government data under the Freedom of Information Act.[4]

Rotenberg draws attention to the peculiar dangers we confront when government simultaneously enlarges its surveillance over our lives and diminishes our ability to monitor that surveillance. This is exactly what has happened, he argues, since September 11. He describes the challenge now for the legal community to "assess these developments and to determine their impact on current law and the rights of citizens."[5] It is to that task that the contributors to this symposium have addressed their efforts.

Professor Daniel Solove opens the first panel discussion with an examination of the danger to our right to privacy that comes when otherwise innocuous bits of personal information are disseminated in the aggregate.[6] He begins by challenging the prevailing view that privacy turns on whether the information at issue is "secret" or "non-secret"; i.e., whether it appears in public records. Instead, argues Solove, privacy should be understood as an expectation of a limit on the degree of accessibility of information.[7] He then goes on to contend that the privacy interest in dissemination of personal information extends beyond potentially embarrassing or harmful information to other, seemingly innocuous pieces of personal information that appear in public records. Though these pieces of information, by themselves, may be harmless, their aggregation paints a "digital biography" of the individual that may be used in a

3. *Id.* at 1123.

4. *Id* at 1123-25.

5. *Id.* at 1134.

6. Daniel J. Solove, Access and Aggregation: Public Records, Privacy and the Constitution, 86 Minn. L. Rev. 1137 (2002).

7. *Id.* at 1141.

number of ways that dehumanize and make vulnerable the individual about whom the data is collected.[8] This is increasingly feasible in today's information age, with records available to most public, government, and private institutions at the click of a button.

Solove's solution is to limit, without prohibiting, access to the information contained in public records. He advocates regulation of specific uses and the exclusion of personal information from public records where possible. Access would, effectively, be limited in such a way as to prevent the dangerous aggregation of personal information. This approach, he argues, would protect the individual's privacy interest while still allowing for appropriate public oversight of government activity through survey of public records, the "transparency" value of public access to records.[9] Additionally, the federal government should impose a baseline to protect a meaningful floor for privacy protection while allowing states maximum latitude in creating stricter protections.[10]

Symposium contributors Edward Janger, Paul Schwartz and Peter Swire narrow the scope of the debate, focusing on recent changes in federal law affecting the privacy of personal financial data. The Gramm-Leach-Bliley Act of 1999[11] (the GLB Act) loosened federal restrictions on mergers and affiliations between various types of financial institutions, including banks, investment companies, insurance companies, and other financial businesses. The idea was that just as consumers should not have to shop in separate stores for meats, vegetables, and bread, they should not have to shop in separate institutions for insurance, investment advice, and bank accounts. Just as we have supermarkets in food, after the GLB Act we have supermarkets for financial services and products. For consumers, there are obvious advantages to this new arrangement in terms of convenience and coordination of financial affairs.

This all sounds unexceptionable until the potential consequences for the privacy of personal financial data are considered. After the GLB Act, comprehensive information about a person's finances is available in a single, readily accessible database compiled by a single commercial entity comprised of the

8. *Id.*
9. *Id.* at 1198-99.
10. *Id.* at 1200.
11. Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

various sub-entities or affiliated entities from which the data was compiled. This compilation of information has economic value, for example, to a marketing firm that might then use the information to make targeted sales pitches to consumers. Because marketing and other firms will be willing to buy your financial information, your convenient commercial conglomerate will find a price at which to sell it.

If the only consequence of this information-sharing is that consumers will get more junk mail to throw away and a few more dinner-hour calls from telemarketers, there would seem to be little to get excited about. But, as Professors Edward Janger and Paul Schwartz point out,[12] there may be a much greater loss than that at issue.

Congress foresaw potential privacy concerns in the new legislation and grafted several privacy measures onto the GLB Act to deal with the problem. First, financial entities must send annual notices to their customers describing their privacy policies. Second, they may freely share their customers' financial information with affiliated companies but may not share the information with outside companies if the subject customer, after notice, objects. That is, customers may "opt-out" of the information sharing otherwise permitted. Third, financial entities must adopt procedures to protect customers' financial data from unauthorized disclosure (to hackers who gain access to databases, for example). Finally, the GLB Act authorizes federal agencies to enforce its privacy provisions (but gives no right of action to individuals to sue for violations).[13]

Much of Janger's and Schwartz's criticism is directed at the first two of these provisions, requiring notice to consumers and the opt-out right. The privacy protections, they argue, have been completely ineffective at preserving financial privacy. Janger and Schwartz cite a survey that found that few consumers recall receiving the notices and a trivial number (0.5% of all banking customers) exercised their opt-out rights.[14]

The interesting question is why consumers have not acted to protect their financial information from widespread disclosure. One possibility is that financial customers just aren't very concerned about the privacy of that data, doubt the risks

12. Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219 (2002).

13. *Id.* at 1225.

14. *Id.* at 1230.

of inadvertent or unauthorized disclosure, and at any rate are willing to make sacrifices in privacy because they want the consumer benefits of information sharing.

Janger and Schwartz offer considerably more plausible reasons for the low-level of opt-out by financial customers. One is that the privacy notices are typically written in complex and legalistic language that many consumers have neither the ability nor the time and patience to wade through.[15] Another is that consumers assume the privacy and opt-out notices are junk mail and throw them out.[16] A third reason for the rarity of opt-out is the "framing effect," the ability of financial institutions to frame the decision for the customer in terms of the costs of opting-out (for example, by warning that a customer who opts-out may not receive valuable offers) rather than in terms of the benefits of maintaining greater control over her own financial data.[17]

One solution might be to reverse the default rule, that is, to require customers to "opt-in" before their financial data can be shared with non-affiliated financial entities. This would put the burden on financial entities to persuade their customers of the benefits of information-sharing. It would seem to enhance individual autonomy because it would maximize the likelihood that individuals would make meaningful choices about the availability of their own financial data.

But this does not go far enough for Janger and Schwartz, who argue for what they call a "norm enforcing default."[18] First, they argue that because of high information costs individuals are unlikely to be competent to choose among various institutions offering complex privacy policies. Second, individual preferences about privacy are themselves a product of legal rules about privacy. So legal rules affirming individual preferences cannot be justified without circularity.[19] To offset the preference-shaping effect of law, legal rules must be set according to some substantive value independent of those preferences. For Janger and Schwartz, the substantive value to be a preserved is "constitutive privacy," that level of privacy important to democratic society. "Particular attention is needed to prevent revelation and use of data that might chill one's underly-

15. *Id.* at 1230-31.
16. *Id.*
17. *Id.* at 1232, 1242-43.
18. *Id.* at 1245.
19. *Id.* at 1250.

ing capacity for decision-making," they argue.[20] Janger and Schwartz argue for a mixed regime of mandatory, non-waivable privacy protections and default rules that set a baseline for negotiations between the customer and the financial institution about how much of the person's financial data can be shared.[21]

This style of argument has become common in legal journals. Individuals, for one reason or another in this view, cannot always be trusted to make good decisions for themselves so certain decisions must be made for them. It is the paternalistic justification for any legal rule that creates non-waivable rights. The irony, if it is an irony, is that a regime designed to enhance autonomy does so by denying individual choice.

Is there a desirable alternative to a norm-enforcing default for financial privacy? One alternative might be to give consumers a contract or property right in their personal financial information, which they can bargain away as they see fit. The available evidence is that individuals might well exact a high price for access to their personal financial data, since polls show Americans regard such information as especially sensitive (akin to the importance they place on medical privacy).

Such an alternative regime might require that consumers be given truthful, non-misleading, easily understood information coupled with a default rule (such as an opt-in right) that encourages meaningful consent to data-sharing. There would still be the problem of dealing with consumer preferences, which are surely shaped in part by existing privacy law. But that problem would also seem to be present in a norm-enforcing regime, which arrives at its substantive values through democratic preferences that are themselves susceptible to the shaping effect of law.

Professor Peter Swire offers the unique and valuable perspective of a person directly involved in the creation and administration of the privacy-related provisions of the GLB Act.[22] From March 1999 to the end of the Clinton administration, he served as Chief Counselor for Privacy in the U.S. Office of Management and Budget. Swire helpfully summarizes the history of the adoption of the financial records privacy provisions.[23] He also draws connections between the financial pri-

20. *Id.* at 1252.

21. *Id.* at 1254-55.

22. *See* Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263 (2002).

23. *Id.* at 1273-94.

vacy provisions and those related to medical records.[24]

Swire concludes that, on balance, the GLB Act "works surprisingly well as privacy legislation."[25] He agrees with Janger and Schwartz that the creation of an opt-out right to avoid data-sharing with unaffiliated financial institutions is inadequate to protect privacy. Instead, Swire would prohibit most data sharing with unaffiliated institutions.[26] Based on the account of the legislative process Swire provides, no serious consideration was given to an opt-in alternative, much less to the hybrid, norm-enforcing default Janger and Schwartz propose.

As to the required privacy policy notices panned by Janger and Schwartz as hopelessly complex, Swire notes that creating the notices required companies to review their own privacy policies for the first time. As a result, many companies altered their policies to make them more protective of financial information and appointed "Chief Privacy Officers" to monitor firm compliance.[27]

Swire proposes a two-tiered approach to the notices under which a simpler, short-form notice would be sent to customers while a more detailed long-form notice would be prepared by the company and available (upon request) to the public.[28]

The second set of privacy issues addressed by this symposium arises out of the Supreme Court's important Fourth Amendment decision from last year, *Kyllo v. United States*.[29] In *Kyllo*, the Court held that the use of thermal imaging technology to monitor a house was a "search" within the meaning of the Fourth Amendment. The government had used the technology to detect heat emanating from a section of a private home, suggesting the occupant was growing marijuana inside. Justice Scalia's opinion for the Court emphasized that where surveillance technology (like thermal imaging) is "not in general public use" the Court must "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[30]

Therefore, where government uses technology not generally in use to monitor citizens' homes it must ordinarily obtain

24. *Id.* at 1278.
25. *Id.* at 1263.
26. *Id.* at 1301.
27. *Id.* at 1316.
28. *Id.* at 1318-26.
29. 533 U.S. 27 (2001).
30. *Id.* at 34.

a warrant before conducting the surveillance. In a world where government's investigative powers include new, ominous-sounding programs like "Carnivore," which allows law enforcement authorities to capture all online information from email to web surfing facilitated by an Internet service provider, *Kyllo* offers some solace to privacy advocates.

It is not a satisfactory answer to a Fourth Amendment question that we should follow the specific intentions of the Framers with respect to a particular privacy claim. The FBI has confirmed that it is developing an Internet surveillance program, code-named "Magic Lantern," that can record every keystroke on a person's computer without the need to physically access the computer. The Framers could never have conceived such a surveillance device since they could not have imagined computers or the system that allows computers to communicate with each other, the Internet. If the Fourth Amendment were understood to prohibit only what the Framers specifically thought it would prohibit in the world of 1791, then privacy is dead. The Court now appears content to adhere to a much broader vision of the Framers' design by trying to tease a broader privacy principle from history.

Professor Raymond Ku argues that the Fourth Amendment is "best understood as a means of preserving the people's authority over government" through their "sovereign right to determine how and when government may intrude into the lives and influence the behavior of its citizens."[31] Thus conceived, the Fourth Amendment is chiefly about preserving the people's power, not protecting their privacy. The corollary to this view is that the Fourth Amendment, in conjunction with the doctrine of separation of powers, ought to be seen as a limit of governmental power, which the Framers saw as the chief threat to liberty.[32]

On this formulation, Ku rejects judicial balancing of the costs and benefits of privacy. For Ku, it is not a judge's function to weigh "the relative value or efficacy of such [investigative] tools against the corresponding loss of privacy and cost to society" but instead to determine whether the people themselves have constitutionally conferred "upon their representatives the decisionmaking authority to conduct such a balanc-

31. Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002).

32. *Id.* at 1338.

ing."[33] This conception seems to require a substantive vision of what the Fourth Amendment protects.

For Ku, this means elevating "the people" to the preeminent role in determining the scope of governmental investigatory power. The Framers, in Ku's view, were less concerned with roping off distinct areas of life (the home, for example) from government surveillance than with limiting the power of government to invade *any* "aspect of life" unless it has "sufficient cause" to do so.

Ku's thesis raises a series of interesting issues. Can courts determine whether government has "sufficient cause" to invade an "aspect of life" without making some judgment about the importance of the particular aspect being monitored? How are "the people" to be empowered by a Fourth Amendment jurisprudence that is developed and applied by courts? Suppose "the people," in the aftermath of events like September 11, want the government to have broad powers of surveillance to prevent similar tragedies in the future? Does the substantive meaning of the Fourth Amendment change with their changing priorities? If the answer to that last question is "no," as one might suspect it is, then in what sense are "the people" really in charge?

While Ku welcomes *Kyllo*'s suggestion that the Court will subject new surveillance technologies to Fourth Amendment scrutiny, Professor Christopher Slobogin sees cause to worry about the decision.[34] Slobogin argues that it should be irrelevant to the Fourth Amendment analysis that a technology is or is not "generally available." Observation of the home, even with technology that is widely available to the public, should be governed by the Fourth Amendment.[35] This analysis comports with the common understanding of what constitutes a search: Even when the police peer into your bedroom with an ordinary, and widely available flashlight, they are conducting a "search."

Slobogin emphasizes the instability the *Kyllo* Court's "general public use" analysis introduces into Fourth Amendment jurisprudence. Technology that seems exotic in one era becomes commonplace in the next. Consider that the zoom camera was not introduced until 1986. Rapid technological changes

33. *Id.* at 1328.

34. Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo's *Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393 (2002).

35. *Id.* at 1397.

make such equipment cheaper and therefore more accessible to the general public. "When that happens," Slobogin writes, "courts will either have to change their stance, manipulate the meaning of the general public use doctrine, or ignore it."[36] These options are, to Slobogin, not "palatable."[37]

The general public use doctrine appears to arise from an underlying privacy principle identified in *Katz v. United States*[38]: The Fourth Amendment protects not all claims of privacy, but only *reasonable* expectations of privacy. The more generally available a surveillance technology is, the less reasonable it is for individuals to expect that others will not use the technology in ways that invade what was previously thought private. Before airplanes, an eight-foot fence around your backyard created a reasonable expectation that nobody would see what you were doing behind it. But if you live under a commercial flight path, with pilots and passengers fully able to look down on you, the eight-foot fence no longer gives you a reasonable expectation that you will be unseen. If reasonableness is the touchstone of Fourth Amendment analysis, it is not difficult to see how it might apply differently in different times.

Unlike Ku, Slobogin emphasizes that the inside of the home is a special place in American law, including the Fourth Amendment. For that reason, he favors an absolute approach to surveillance of the home: "Peering into the home by government officials, at least when it relies on enhancement devices, should *always* be considered a Fourth Amendment search."[39] For Slobogin, all government surveillance of a home would require probable cause, and a warrant in non-exigent circumstances. In response to concerns that this broad definition of "search" would seriously undermine police investigative work, Slobogin offers to broaden the definition of "probable cause."[40] One wonders whether this peace offering to law enforcement might constitute a one-step-forward-one-step-back result for privacy advocates. Slobogin's approach makes the ubiquity of the surveillance-enhancement device irrelevant, but at the cost of relaxing the standard for justifying a search.

Professor Bandes agrees with Ku's characterization of the current Fourth Amendment debate as one about power, not

36. *Id.* at 1413.
37. *Id.*
38. 389 U.S. 347 (1967).
39. Slobogin, *supra* note 34, at 1108 (emphasis added).
40. *Id.* at 1426-27.

privacy, but disagrees with the significance Ku attaches to the advent of new technologies.[41] According to Bandes, treating the issue of technological advances and whether they intrude on our expected sphere of liberty as an independent inquiry deflects us from the truly critical inquiry: whether the police action in question is offensive to a free and open society.[42] This inquiry hinges on a contemporary understanding of what balance the Fourth Amendment ought to preserve, which reunites her with Ku's disdain for the "Framers' privacy" as a guiding light.[43]

Bandes sees the public use doctrine as an illusory basis for safeguarding our privacy under the Fourth Amendment. The danger to be curbed is *police* use of technologically advanced surveillance equipment, so the public availability of that same technology is of little consequence to the inquiry. In addition, she joins Professor Slobogin in asserting that the general use doctrine affords us only the amount of privacy that is available from the public at large, which wanes every day as we become more technologically advanced and technology becomes more available.[44]

The third area of focus for this symposium, and the one that draws the sharpest dispute among symposium participants, concerns the privacy of personal medical information. In the Health Insurance Portability and Accountability Act of 1996[45] (HIPAA), Congress authorized the issuance of federal regulations governing the privacy of personal medical data handled by covered entities, such as medical practices and hospitals. After receiving 52,000 public comments on a set of proposed guidelines, the Clinton administration announced the final rules in December, 2000. In April, 2001, the Bush administration announced the guidelines would take effect largely as drafted by Clinton's Department of Health and Human Services. This sequence of events, along with summary of the HIPAA privacy regulations themselves, is helpfully described by Professors Lauren Steinfeld and Peter Swire in their joint contribution to the symposium.[46]

---

41. Susan Bandes, *Power, Privacy and Thermal Imaging*, 86 MINN. L. REV. 1379, 1384 (2002).

42. *Id.* at 1384-85.

43. *Id.* at 1388.

44. *Id.* at 1391.

45. Pub. L. No. 104-191, 110 Stat. 1936 (1996).

46. Peter P. Swire & Lauren B. Steinfeld, *Security and Privacy After Sep-*

It is instructive to compare the HIPAA privacy regulations governing medical data with the GLB Act rules governing financial data. Both contain a notice requirement, mandating that covered entities give their customers information about their internal information privacy practices. Both require covered entities to develop policies to safeguard information from inadvertent or unauthorized disclosure. One seemingly significant difference between the two is that whereas the GLB Act sets an opt-out default for the protection of financial privacy (allowing covered entities to share financial data unless the customer objects), the HIPAA regulations set an opt-in default for the protection of medical privacy (generally barring covered entities from sharing medical data unless the customer consents). This difference, however, turns out to have little practical significance in the actual application of the HIPAA privacy regulations.

Professors Lawrence Gostin and James Hodge, in an especially provocative contribution to the symposium, argue that the HIPAA regulations go too far in shielding individual medical privacy.[47] As a consequence, HIPAA may sacrifice important public goods like health research, public health, the administration of justice, and law enforcement. Unauthorized disclosures of personal health information are sometimes needed, they argue, as in cases where infectious diseases must be reported to state health departments and where persons at significant risk of harm must be warned of danger.[48]

As an alternative to an emphasis on individual autonomy as the dominant factor in health information privacy analysis, Gostin and Hodge favor an explicit balancing approach. Under their model, private and public interests in disclosure would be weighed against each other. "Thus," they write, "where the potential for public benefit is high and the risk of harm to individuals is low, we suggest that public entities should have discretion to use data for important public purposes."[49] By contrast, where disclosure is "unlikely to achieve a strong public benefit, and the personal risks are high, individual interests

tember 11: The Health Care Example, 86 MINN. L. REV. 1515 (2002).

47. Lawrence O. Gostin & James G. Hodge, *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439 (2002).

48. *Id.* at 1441.

49. *Id.*

in autonomy should prevail."[50] The personal risks of disclosing individual medical information include stigma, embarrassment, discrimination, and loss of patient trust and cooperation with health care professionals.

Gostin and Hodge candidly acknowledge that their model will "entail a certain diminution of autonomy," but insist that this cost is worth the benefits in terms of improved clinical care, research, and protecting public health that arise from greater information-sharing.[51] Individuals have a strong interest in personal privacy, to be sure, but they also have a strong interest in a healthier and more secure society. Thus, the communal good in information access can be recast as an individual good.

Gostin and Hodge suggest that we should avoid the propertization of individual medical data because it will too severely restrict the flow of needed information.[52] Their model for medical data is thus similar to the one offered by Janger and Schwartz for financial data: Both approaches reject giving individuals general property and contract rights in the control of their personal information. Moreover, both sets of authors reject an individual choice approach in favor of a substantive value they identify. For Janger and Schwartz, that value is driven by the needs of a democratic polity to promote the capacity for individual decisionmaking. For Gostin and Hodge, that value is the communal good. Both sets of authors are willing to commandeer individual information for the purpose of serving the relevant identified norm.

The difference between the two models is in the preferred outcomes: Janger and Schwartz commandeer the information in order to protect it from disclosure, whereas Gostin and Hodge commandeer the information in order to make it available for disclosure. Janger and Schwartz fear that if individuals are given complete control over their own information, *they will bargain away too much of their privacy*. Gostin and Hodge fear that if individuals are given complete control over their own information, *they will bargain away too little of their privacy*.

In practice, the written informed consent required for the disclosure of personal health information by the HIPAA privacy

50. *Id.* at 1442.
51. *Id.*
52. *Id.* at 1453.

regulations "is neither informed nor consensual."[53] The informed consent is not truly informed because patients cannot know *a priori* precisely what future medical information they are being asked to make available for disclosure. It is not truly consensual because providers condition treatment on whether the patient signs the consent form. This choice is colorfully described by Minnesota Attorney General Mike Hatch as a "sign or die" provision.[54]

Where Gostin and Hodge fear the HIPAA privacy regulations are overprotective of personal medical information, Hatch argues it is underprotective. Hatch claims that Gostin and Hodge "reject the inherent importance of privacy in our culture."[55] There is little need, in his view, to have patient identifiers (e.g., the patient's name or social security number) attached to medical information disclosed to government, researchers, and insurers. That information can be used to deny a mortgage application, a job, or an insurance policy. Of course, the fact that the information could be used for those purposes shows that it has some value to those who would use it against the individual. It is surely relevant to a life insurance application that the applicant is being treated for a fatal disease.

Hatch highlights a risk not emphasized by the other contributions to the symposium. The more widely available the information, the more likely it will be misused or inadvertently disclosed. Consider that the Medical Marketing Service offers for sale fifty lists of people suffering from various medical conditions, including clinical depression, yeast infections, and diabetes. Consider, too, that an employee of the state health department in Florida released the names of 4000 AIDS patients on the grounds that he was performing a public service.[56]

Hatch contends that the HIPAA privacy regulations have less to do with "communal good" than with a standard public-choice story. The regulations, he argues, reflect the interests of lobbyists and commercial interests who have significant financial stakes in obtaining individual medical information. This has resulted in agency capture by lobbyists: "The proponents of HIPAA represent a closely connected liaison of government

53. *Id.* at 1467.

54. Mike Hatch, *HIPAA: Commercial Interests Win Round Two*, 86 MINN. L. REV. 1481, 1485 (2002).

55. *Id.* at 1486.

56. *Id.* at 1491.

agencies, pharmaceutical companies, law enforcement agencies, medical device manufacturers and marketing concerns. Their success in getting HIPAA adopted rivals the clout of the military industrial complex at the height of the Cold War."[57] This is strong stuff.

Alongside Hatch, Professor Peter Jacobson views privacy as the paramount interest in the HIPAA story.[58] Jacobson's assessment of the Gostin and Hodge model is that, while it correctly assigns significant value to the communal benefits of health information disclosure and would fit well within the HIPAA framework, it is suited only for a very narrow and finite set of circumstances and is impractical in application. Application of the Gostin and Hodge approach is clear when the communal interest is extreme—for example, protection against bioterrorism—but offers little guidance in cases where the communal interests pursued are more graduated. Further, Jacobson takes issue with Gostin and Hodge's default protection of communal interest. It would appear that this default means that any uncertainty in application of the Gostin and Hodge model will be resolved against a claim of individual privacy.

Jacobson would, instead, implement a rule of reason analysis patterned after antitrust law to determine when the communal interest in disclosure of private health information outweighs the individual privacy interest. The basis would be a "need to know" standard, taking into consideration the patient's best interests.[59] Most significantly, however, and in direct contrast with the Gostin and Hodge approach, the patient's privacy interest would be the default position in cases where the balance between communal and private interest is not obvious.[60] This default would guide the reasonableness test to which covered entities would be held when they seek health records.[61]

Hatch, Jacobson, Steinfeld and Swire all warn that the Gostin and Hodge model of information sharing will erode patients' willingness to speak freely to their medical providers, undermining public confidence in the medical establishment

57. *Id.* at 1494.

58. Peter D. Jacobson, Medical Records and HIPAA: Is It Too Late to Protect Privacy?, 86 MINN. L. REV. 1497 (2002).

59. *Id.* at 1513.

60. *Id.*

61. *Id.* at 1514.

and therefore undermining public health. This suggests there is a communal good in preserving individual privacy.

Still, there may be less to this disagreement than first meets the eye. Though participants disagree on the appropriate theoretical emphasis in the protection of personal medical information, they do not identify any specific instances of disagreement. That is, Gostin and Hodge do not give any examples of circumstances in which they would permit the disclosure of medical information not already permitted by the HIPAA privacy regulations. And Steinfeld and Swire give no examples of circumstances in which they would prohibit disclosure but Gostin and Hodge would permit it. But wait awhile; the day is just dawning on our new world of privacy law.