2004

The International Privacy Regime

Tim Wu
Columbia Law School, twu@law.columbia.edu

The International Privacy Regime

> "If a privacy official flaps his wings in Brussels, can it set off a hurricane in San Francisco?"
>
> Tim Wu[1]

Introduction

In the month of April 2004, the state of privacy shifted in different ways in different parts of the world. In Shanghai, China, government officials announced the installation of video cameras in each of the city's more than 1300 internet cafés. The cameras actually watch you as you read your personal email, surf web sites, or chat with friends. According to city official Yu Wenchang, the surveillance program helps protect youth from pornography and "superstitious" web sites by allowing the government to "spot illegal activities immediately." Big brother, he might well have said, is watching.[1]

At the same time, across the Pacific, Google officials announced their latest invention: "Gmail." Gmail, Google says, gives users enough storage room to keep their emails more or less forever. But there's a catch: every message you send and every message you receive is read by a highly intelligent robot, who guesses what kind of advertisements you might find interesting. Say you're discussing a trip to Spain with your secret lover: Google will sidebar advertisements for hotels and airfares. It's only a robot, not a human, reading what may be your deepest secrets. Nonetheless, some people find the whole idea unnerving.

Both stories are about private information. The first has Chinese officials reading your email, the second, Google's robots. Both flip important presumptions. In China the internet cafés once meant freedom; they are increasingly yet another point of control. Gmail makes email, for many people a most secret place, a little less so. But both privacy concerns are countered to different degrees by consent: you don't have frequent the internet cafés, nor is anyone required to use Gmail. As a Gmail user myself, I find the robots harmless. Yet the consent arguments don't satisfy everyone. As Brad Templeton, chairman of the Electronic Frontier Foundation, wrote in a perceptive essay on Gmail, "the fear that computerized scanning of our e-mails (to display ads or filter out spam) will result in actual harm is largely baseless. But even irrational fears affect our freedom."[2]

---

[1] Associate Professor of Law, University of Virginia.

That's the debate. What did the Law have to say? In another twist and across another Ocean, the greatest regulatory threat came from Europe, and it came to the American robots, not the Chinese officials. Within weeks of announcing Gmail, Google was surprised to find legal complaints filed against it in the European Union and various European countries. On April 19, 2004, an English group named Privacy International filed complaints in the EU, France, Germany, the Netherlands, Greece, Poland, and many other countries. It demanded that regulators "investigate the Gmail service with regard to compliance with Data Protection" and, if they found compliance wanting, "that an order may be made to prohibit the export of personal data to Google."[3]

What's going on? If internet privacy is supposed to be primarily "self-regulating," why do privacy advocates look to Europe to police an American email service run by a private company? Conversely, isn't this all backward: why doesn't anything or anyone protect Chinese citizens from far more unnerving invasions of their privacy?

These stories show that, today, no one can speak usefully about law and privacy without understanding the *de facto* international privacy system. As Peter Swire first wrote in 1998, privacy has joined one of many areas of law understandable only by reference to the results of overlapping and conflicting national agendas.[4] What has emerged since 1998 as a *de facto* regime is complex. Yet based on a few simplifying principles, we can nonetheless do much to understand it and predict its operation.

First, the idea that self-regulation by the internet community will be the driving force in privacy protection must be laid to rest. The experience of the last decade shows that nation-states, powerful nation-states in particular, drive the system of international privacy. The final mix of privacy protection that the world's citizens receive is disproportionately dictated by the choices and preferences of powerful nation-states and their respective effects on giant and small targets (in Swire's terminology, "elephants" and "mice").

Second, traditional conflicts analysis can help explain and predict the future course of privacy analysis. Privacy regulation can be understood as a species of information regulation to which companies and individuals will respond in predictable ways. The analysis here shows an international privacy system that has fractured into three distinct regulatory patterns. Mainstream privacy, or *transactional privacy*, has become dominated by the rule of the most restrictive state, a pattern familiar to other areas like the world's regulation of competition (antitrust). Conversely, the problem of *information theft* has been pushed by the international system toward a kind of a race to the bottom, or to the least restrictive rule. Most akin to international piracy (the kind on boats), it

is a familiar problem to international law that will nonetheless take considerable political will to reverse. And finally, while there is a potential for the international system to influence how governments handle the privacy information of their own citizens, the direct collision of interests have limited the extent to which governments police one another.

What does this mean for Americans? First, it suggests that any normative view of privacy must take into account the descriptive fact that much of the privacy policy that affects Americans will be set overseas. Second, it suggests that those Americans who want more government privacy protection should focus their efforts on convincing significant economic units, such as countries or U.S. States, to enact strong and extraterritorial privacy legislation. Finally, it suggests that those who believe that less governmental regulation is appropriate cannot simply point to self-regulation, but must seek "countervailing" or claw back legislation.

The International Privacy System

Consider the following, expressed by the TRUSTe web site, a program of voluntary privacy certification:

> Unless there is global harmonization of privacy laws, government oversight is seriously challenged. A Web site can easily be located outside the jurisdiction of a nation-state and thus not be bound by its laws.[5]

What is interesting is that TRUSTe has got things almost exactly backward. It is true that the ease of transferring digital information has made abuse of privacy easier, and cheaper. Cheap information has brought attention to privacy policy for the same reasons that cheap crack cocaine made drug policy an issue in the 1980s[6] and that cheap food has contributed to the American obesity epidemic.[7] Cheapness, in short, has unintended consequences.

But global information networks have also made governments more, rather then less, capable of regulating outside their borders. There are two reasons. The first and primary reason is that the targets of regulation, like the flows of information that are their business, are increasingly multinational. This is the story of .NET Passport discussed below. If the target of a law operates in multiple jurisdictions, a nation will sometimes influence the conduct of the multinational across jurisdictions. The second is slightly more legalistic: the internationalization of information flows has justified claims of extraterritorial regulation premised on domestic effect. As the examples in this paper demonstrate, the main example is well known among scholars, if not the general public: that much online privacy policy is today influenced heavily by

extraterritorial European Union regulation. But the example of the European Union is merely evidence of a broader phenomenon.

It is important to emphasize that legal internationalization is certainly not unique to privacy regulation. It follows patterns seen in other legal fields, and its consequences are not unpredictable. Antitrust law is perhaps the clearest example. When insurers in London agree on insurance policies, they need to keep American antitrust law in mind, thanks to the Supreme Court's decision finding the practices of the London insurance industry within the jurisdiction of the Sherman Act.[8] As Microsoft designs its latest operating system, it must keep in mind European, American, and probably Japanese competition law. Antitrust has been internationalized for at least the last fifty years thanks to the internationalization of commerce. And while it has certainly complicated the study of antitrust law, it has not by any means rendered the law of the nation-state irrelevant.

Yet saying that nations have seen their privacy laws enjoy greater extraterritorial effect does not answer the most important question. Will it be the country that cares least about privacy – say, China – or the country that cares most – say, Germany – that sets the default rule for the entire world? Answering this question requires the more complex model introduced next.

The Governance of Private Information

Privacy regulation is most easily understood as a species of information regulation. Typical privacy laws are governmental rules concerning how information may be used,[9] with or without permission of a given "owner." In this respect, privacy regulation is analytically analogous to other forms of communications regulation, such as libel, copyright law, and indecency regulation.[10] It is for this reason that the rise of a universal information network, the internet, has changed a set of questions answerable by reference simply to territory into a more complex international puzzle.

Privacy regulation is distinguished by strong, indeed fundamental differences of opinion between nation-states. Much information regulation, like copyright, exists in a rough consensus among economically powerful nations, as embodied in international agreements such as the Trade Related Intellectual Property Agreement, TRIPS. But privacy questions seem to touch closer to the nation's psyche, and even culturally similar nations differ profoundly over what they consider "adequate" in the regulation of privacy. Americans, by reputation, see privacy as a negative freedom, that is, principally a protection from government. Americans, or at least Congress, are wary of government restraints on commerce practiced in the name of privacy regulation. Europeans, also by

reputation, care more than anyone else in the world about the sanctity of private information and want greater policing of the abuses of the private sector. To take just another example, scholars of Chinese culture, struggling to find the meaning of privacy in the Chinese context, have gone so far as to claim that the Western conception of privacy lacks meaning altogether.[11]

Conflicts analysis arises when two or more jurisdictions share information freely, but have different privacy rules. Consider two jurisdictions, A and B, with different privacy rules, lenient and strict:

A	B
Lenient	Strict

In a world where information is not shared, each exercises authority concurrent with its territorial jurisdiction. But if each state both shares information freely, and wants its rules to apply (if privacy is a mandatory rule, in conflicts jargon), which law will in fact govern?

A		B
Lenient		Strict
Citizens<----------	Free	----------> Citizens

The question is whether the rule will be the rule of the lenient or strict country. The former we call the rule of the Least Restrictive, and the latter, rule by the Most Restrictive. While a complex question, whether the default outcome will be the Least or Most Restrictive rule can be expected to depend on just a few factors.

Existing scholarship on internet privacy has tended to focus on the *size* of the regulated entity as determinative of whether a given form of privacy regulation will be effective. This is most evident in Peter Swire's work. In 1998 he introduced the metaphor of "elephants" and "mice," predicting that privacy regulation would generally be effective against the former but not the latter.[12] In other work, Gregory Shaffer, concentrating mainly on the effects of EU regulation on large U.S. firms, predicts that the EU will generally push the United States toward more privacy protection.[13]

These authors are correct to suggest that larger entities are easier to regulate, but the observed size of firms in certain types of transactions is itself dependent on other factors. While the international privacy system is new, it follows several dividing lines familiar from international conflicts analysis.

First, much of the international privacy system is shaped by a distinction between the behavior in the model of an international transaction, on the one hand, and an international crime or tort, on the other. The relevant distinction between the two is the difference between regulating *consensual* and *non-consensual* relationships. For reasons explained below, the elephant / mouse pattern may emerge to fit this distinction.

The transaction / tort distinction matters because it determines a factor critical to conflicts analysis: who the *initiating* party is, or who gets to choose the governing legal regime. In crimes or non-consensual transactions, the firm initiates the transaction, and it is its choice that dictates the relevant law. Because firms usually prefer less regulation, this drives a race to the least restrictive rule.

Conversely, for consensual relationships, it is the consumer who initiates the transaction. This puts the consumer in a position to choose the governing law, and the consumer we can assume will choose the strict regime, that which protects his or her rights. Now it may seem a mere fiction that the consumer is actively choosing a legal regime, and of course it is unlikely that the consumer is consciously doing so. But what the consumer does do is decide to trust large, well-known firms with his or her private information. This choice can amount to a choice of legal regime: for if consumers all choose large companies that are regulated by the strict rule, they have in effect made the strict rule the default rule.

From this we can conclude that the nature of the transaction will influence whether the default international privacy rule will tend toward the least or most restrictive in the first place. But from this initial default, set by the choice of the transacting parties, comes a second phase, wherein the specific will of nation-states is expressed. Nation-states, if they take an interest in the matter, may try and reverse the outcome default most or least restrictive rule.

Contests between states to alter default international rules are a familiar phenomenon to scholars of international law. Countries that resent the legal influence of other countries can and do enact legal "countermeasures" or "claw backs." For example, the United States and the rest of the world disagree profoundly on what to do about Cuba. So every time the United States passes laws that threaten to punish foreign companies who deal with Cuba, Europeans and Canadians have reacted with reciprocal laws designed to negate the effect of the American laws.[14] Such dynamics can also shape international privacy regulation.

Three Patterns of International Privacy Regulation

Much of the rest of this paper is dedicated to understanding how this two-stage process has played out for privacy regulation. What we find is an emerging split among different types of privacy regulation. In what follows, consider three emerging categories of regulatory problems:

1. Breach of Trust / Transactional Privacy. Much information is transferred to others in consensual transactions. The unwanted behavior occurs when that party then does things that you would prefer they not do with your information. For example, if your doctor knows you have a embarrassing disease, it might be your preference that he not tell everyone. Similarly, a bank might sell your personal information to third-party solicitors who then call day-and-night. In this category are laws that try and control what third-parties do with information to create a correspondence between what you want and what they do.

2. Information Theft / Protective Privacy. A different category of privacy problem arises when your information is taken without consent and used in abusive ways. Someone who steals your wallet might gain access to your credit card number and rack up unwanted bills. Information theft is primarily a matter of security-regulation, and laws preventing information theft penalize such conduct.

3. Governmental Abuse / Constitutional Privacy. A final category is the misuse of private information by government entities.[15] Here, as in transactional privacy, the actor is known, yet like information theft, the exchange of information is non-consensual. You do not have a choice as to whether to tell the government how much money you made when paying your taxes, for example, or whether or not you want the police to listen in on your telephone conversations.

In each of these areas, recent experience has given us some guide as to what results the international privacy system will yield.

Transactional Privacy & the European Rule

In the spring of 2002, European Union investigators summoned America's Microsoft Corporation to Brussels. It was a familiar path for a company who had already spent years wrestling with European Competition authorities. This time, however, it was privacy investigators from the "Article 29 Data Protection Working Party" who came calling.

The European concern was Microsoft's new ".NET Passport" program.[16] Anyone who uses the web knows that remembering dozens of different emails

and passwords can be a pain. .NET Passport was designed to provide users with virtual "digital identification" to make navigation among password protected sites near-automatic. But the operation of a digital ID system necessarily means the transfer of a lot of personal information. The European privacy officials in the Article 29 Party wanted to know a lot more about how Microsoft was collecting user data and what it doing with it.[17]

Under what legal authority was the EU acting? The European Union has the world's broadest and most stringent data privacy laws. A general European Directive* on data protection was passed in 1995 and implemented in 1998.[18] Its breadth is remarkable. In addition to its geographic scope, discussed in a moment, it regulates not individual industries piecemeal (the American approach) but *any* "data controller," that is, anyone who "processes" the data he or she collects. This has meant, for example, that the law has even reached informal social groups. For example, in 2003, a Swedish woman named Bodil Lindqvist was fined $450 for posting personal data about fellow parishioners without consent.[19] The EU directive even reaches church groups.

For all data controllers like Microsoft or Ms. Lindqvist, the Directive imposes three relatively stringent requirements: duties of notice, fidelity, and proportionality. Notice means that controllers must tell consumers why they are collecting personal data, and receive "unambiguous" consent. Fidelity means that once data is collected, it must be used for the purposes stated, and not redirected to other purposes. And proportionality requires that the data collected has a reasonable relationship to the purposes for which it is collected. It must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."[20] To these basic requirements the Directive adds extra protection for "special information," namely, "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and ... data concerning health or sex life."[21] It was this latter provision that landed Ms. Lindqvist in trouble. She was fined after revealing to the world the "sensitive" information that another church member had injured her foot and would be taking time off from work.

But what really makes the European Union law controversial is its breadth of geographic scope, which can be fairly described as aggressive. Article 4 of the European Directive[22] mandates that Members' data protection laws shall apply not only to companies established in Europe, but also to any company that makes use of data processing "equipment" or "means" in Europe, and any company that may be reached by virtue of public international law. This is a

* A Directive is a form of European Union law that creates a set of rules and then obliges all EU member states to pass laws implementing those rules by a certain date.

broad scope that has been interpreted by European officials to reach nearly any company that collects information from European citizens.[23]

So it was under the authority of the Directive that Microsoft met the European investigators. Some of the EU's concerns would be familiar to Americans, like Microsoft's failure to give proper notice of what the information would be used for. Others were distinctly European, like the complaint that Microsoft was collecting more data than it needed for the purposes of the program, violating the European sense of proportionality.[24] The two sides talked, and by January 2003, Microsoft and the EU had an agreement. Microsoft agreed to make what the European Commission called "radical" changes for how Passport manages user data, including much more notice, and much more user control over how data is shared.[25]

Microsoft's decision reflects an economic judgment and was a foregone conclusion. The European market is obviously too large for Microsoft to decide to ignore. But perhaps most interesting of all, Microsoft decided to implement its changes to .NET Passport globally, not locally.[26] As a result, whether you're in Auckland, Timbuktu, or somewhere in between, when you use .NET Passport, you use a product ironed into shape by the European privacy authorities. .NET Passport was regulated on behalf of Europeans, but the regulations are in effect on behalf of the world.

What the .NET Passport story demonstrates is the potential for the restrictive rule to act as the effective rule of the network for individual companies. Here, Microsoft, an American company, is regulated by European privacy laws, based on the fact that it serves European customers. For Microsoft, for many questions of transactional privacy, the *strictest* privacy laws become the default law of the network.

What general conditions make regulation of transactional privacy, like the example of the EU and .NET Passport, the most restrictive rule? First, and fundamentally, the regulation of transactional privacy is the regulation of known parties. Unlike the regulation of information theft (model 2), the regulation of transactional privacy, by its nature, is the regulation of a consensual relationship, usually a contractual relationship. You *know* you're giving your information to Paypal, Microsoft, the New York Times, or whomever. It is sometimes said that the only difference between contract and tort law is that in tort you don't know in advance who is going to crash into your car. The regulation of transactional privacy is the regulation of contract, and can advantage the European Union or any other strict jurisdiction that knows who the targets of its laws are.

Second, it is banks, airlines, and major companies, large entities, who are trusted with the most valuable personal information. These are Swire's elephants: entities likely to be responsive to the threat of European enforcement, either because of assets or a physical presence in Europe, or simply fear of being arrested when traveling to Europe. Territorial enforcement is therefore that much more likely to be effective.

Information Theft & Spam

In that same April 2004 yet another serious problem of privacy regulation continued its course. That's the problem of spam: and there few problems of failed information regulation that are clearer. Spam's source is a lack of control over personal information, for if spammers weren't able to harvest millions of email addresses, there would be no spam problem. During this same month of April, spam levels reached an historic high, comprising a full 67% of the emails sent on the network. The statistics, while increasingly familiar, are no less depressing: $10 billion per year spent by ISPs fighting spam, and some of the first reported decisions to abandon email because of the spam problem.[27]

But that April also brought good news for those who despise spam. For the first time the power of the United States Government reached malignant spammers. Four men in Detroit were arrested for violating the brand-new CAN-SPAM Act of 2003.[28] It, among other things, makes it illegal to send an email with a fake return address,[29] which is what landed Daniel J. Lin, James J. Lin, Mark M. Sadek, and Christopher Chung in jail.

Yet whenever spammers are arrested or sued, the same question arises: What can the United States or other powerful countries do to stop spamming or any other form of information theft if it moves overseas? While there are measures that can be taken, it remains that this category of problem—information theft—starts from a different baseline. The default rule can be the rule of the least restrictive state in the world, the state chosen by the thief. And since many countries do nothing at all to regulate junk email in particular or information theft in general, the international system exacerbates the challenge.

From the perspective of international law, however, spammers represent a familiar problem. Consider the following description: "a well-defined offense condemned by all nations, committed by private actors ... that [takes] place... where enforcement is very difficult; and harm[s] the economic interests of many nations ...."[30] It sounds like information theft or spam, but it is Eugene Kontorovich's description of piracy, an age-old problem for the international system.

The problem of information theft has many parallels to piracy, and information thieves are probably a better successor to the label "pirate" than the copyright infringers who have inherited the title. Both follow streams of commerce and transportation, taking advantage of weak spots in nation-state power, whether the high seas or the open networks. Spammers and pirates prey on the weak, and disrupt otherwise predictable transit systems. And, in their time, they are hated by all, known as *hostis humanis generis*, or the enemy of all mankind.

Piracy was and still is a challenge for the nation-state, but there are ways of coping with pirates that can be well adopted to the problem of information theft. Now it must be conceded that nation-states are at only the earliest stages of regulating domestic spam and information theft, as the CAN-SPAM story shows, let alone at the advanced stage of regulating international problems. The piracy model offers clear lessons for the future.

The piracy model would dictate, first, the passage of uniform and severe criminal laws among cooperating countries. Piracy, though akin to robbery, was historically punished by all nations the same way: death. This simplified administration and reduced conflict between countries. While a death penalty for information thieves may be extreme, uniform and severe criminal laws are not.

Yet the problem of enforcement will remain, particularly given non-cooperative countries. One important tool used against piracy was and is "universal jurisdiction." As *hostis humanis generis*, spammers are subject to being caught, tried, and punished based only on their activity and regardless of nationality or link to the local territory. The prospect of such punishment further deterred piracy. Other efforts, consistent with the discussion in the last section, are measures taken against countries that become havens for information thieves.

Again, nation-state action against international problems of information-theft and spam is only in its earliest stages. Some of the ideas described here are being pushed, interestingly, by private actors. Microsoft devotes serious resources to the international fight against spam (which shows privacy advocates that your enemy's enemy is your friend). Microsoft has filed lawsuits in the United States and United Kingdom, and has led a campaign to enact anti-spam laws in East Asia so it can sue spammers there too.[31] The point is that nations have in the past battled parasites who feed on international streams of commerce, and they have methods to do so again.

Model 3: Government

When the Chinese Government installs cameras in internet cafés, no one denies that it's an abuse of privacy, but nothing outside of China is done about it. We think we know why: the Chinese government is sovereign over Chinese citizens. It would be difficult if not impossible for other countries to try and pressure the Government to change how it regulates privacy. Right?

Not entirely. First, there is one international system meant to control how governments treat their own citizens, namely, human rights law. And indeed, the major human rights treaty, the International Covenant on Civil and Political Rights, signed and ratified by nearly every country in the world, contains protections for privacy. Article 17 of that Covenant reads:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

However, it would be fair to say that this Article has not had a tremendous effect on the privacy practices of nation-states. For one thing, it prohibits "unlawful" or "arbitrary" interference with privacy, presumably allowing "lawful" interference. For another, enforcement is a particularly scarce commodity in the human rights field. This provision of the Covenant is hardly an enforcement priority of any of the various entities who try to monitor human rights, given patterns of far more egregious abuse.

But if you try to take from this the general rule that States cannot or do not change how other governments treat the privacy of their own citizens, you'd be wrong. Governments do, with some success, try to change how other governments regulate their own subjects, at least when they want to.

The leading example is the notorious Article 25 of the European Directive. Article 25 is a threat: it says to other countries, either adopt adequate data privacy protection for individuals, or face a ban on transfers of data from the European Union. Textually, Article 25 sets out a ban on all transfers of data to countries that fail to maintain less than "adequate" protection for privacy.[32] It shows how far countries can go when they try and push each other around.

The Article 25 has much in common with other sanction regimes. When the United States blocks travel and economic transfers to Cuba or Iran premised on inadequate protection of human rights, it is doing exactly what Europe is doing for privacy rights. The approach has some similarities to an American law: the intellectual property "special 301."[33] That law obliges the U.S. Administration to make an annual assessment of the legal regimes of other countries to determine whether they have been good or bad in their protection of

intellectual property. Countries who have misbehaved are threatened with unilateral trade sanctions. Both Article 25 and similar U.S. unilateral regimes are efforts to set up a closed community for which entry is premised on good behavior. Both are ultimately efforts to make the laws of other countries more like the EU or the United States, respectively.

The potential consequences of Article 25 are dramatic. A ban on all data transfers between Europe and even Russia would bring economic consequences, let alone a ban on all data transfers to the United States or Japan. For that reason, when the European Directive came into force in 1998, the U.S. Administration and the European Commission went into immediate, high stakes negotiations, since neither Europe nor the United States actually wanted a ban on data transfers across the Atlantic.

What resulted was an uneasy truce that reflects the economic power of each side. The United States did not actually pass new laws that would increase privacy protection. Instead, the Commerce Department set up a voluntary program wherein companies would agree to certify their compliance with a rough approximation of the requirement of the European rules. So certified, they would, in theory, satisfy Europe's requirements, and be subject to American enforcement should they fail to live up to their requirements. In 2000, the European Commission, despite reservations, agreed to find that after setting up the American safe-harbor program, the United States had successfully implemented "adequate" data privacy protection.[34] This conclusion warded off the disastrous possibility of a data embargo on the United States.

If the meaning of the safe-harbor agreements seems unclear, it is. The significance of the safe-harbor agreement, while much discussed in the privacy literature, may be greatly overrated (as Joel Reidenberg argues).[35] It is probably best understood simply as an agreement to waive Article 25 with respect to the United States. In other words, the European Union will not create an embargo on data transfers to the United States. But that doesn't mean that Europe won't influence U.S. privacy policies, as the .NET Passport and the Gmail stories show. The jurisdiction of the Directive (through Article 4, discussed above) still reaches many American companies. What the safe-harbor story shows is that the European Union is ready to regulate Americans, but not America.

Conclusion

Many Americans would be surprised to learn that the first and perhaps last word on Gmail's legality will be supplied not in Washington D.C. or Silicon Valley but in Brussels. Some, in the 1990s, expected a collapse of nation-state sovereignty with respect to privacy. It hasn't happened. Instead, there's been a

complicated shift, making the European Union the most influence voice in global privacy regulation, in part because it seems to care the most.

The international privacy regime must particularly be understood by privacy advocates on every side of the debate. As the work here as shown, much can be accomplished by restrictive rules adopted by economically significant markets. In addition to the role already played by Europe, this suggests a rule for political strategies that focus on entrepreneurial U.S. states or nation-states, with an interest in setting a world rule. Conversely, those who take privacy to be already over-regulated need to work to achieve claw-back, or defensive laws that protect locals from extra-territorial privacy regulation.

The consequences of international private law are sometimes surprising. It may, for example, make more sense for Americans concerned about their privacy to trust their information with Microsoft, than, say Sun, because they know that Microsoft is directly governed by European law. Such unusual results are many more will be the future of the international privacy regime.

---

[1] *See China Launches Web 'Big Brother,'* THE AUSTRALIAN, Apr. 22, 2004, *available at* http://www.theaustralian.news.com.au/common/story_page/0,5744,9355931%255E1702,00.html.

[2] Brad Templeton, *Privacy Subtleties of GMail*, *at* http://www.templetons.com/brad/gmail.html.

[3] Complaint filed by Privacy International with privacy and data protection regulators of France, Germany, the Netherlands, Greece, Italy, Spain, Czech Republic, Belgium, Denmark, Sweden, Ireland, Portugal, Poland, Austria, Australia, and Canada along with the European Commission and the EU Commissioners Internal Article 29 Data Protection Working Group (Apr. 19, 2004), *available at* http://www.privacyinternational.org/issues/internet/gmail-complaint.pdf.

[4] *See* Peter Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991 (1998).

[5] The TRUSTe Story, Building Trust Online: TRUSTe, Privacy and Self-Governance, *at* http://www.truste.org/about/truste/about_whitepaper.html.

[6] *See* EDITH FAIRMAN COOPER, THE EMERGENCE OF CRACK COCAINE ABUSE (2002).

[7] *Cf.*, THE COSTS OF CHEAP FOOD 2 (Inst. for Agric. and Trade Policy ed., 2003).

[8] *See* Hartford Fire Ins. v. California, 509 U.S. 764 (1993).

[9] For this approach, see Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

[10] *Cf.* Timothy Wu, *Copyright's Communications Policy*, MICH. L. REV. (forthcoming 2005); Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354 (1999), *available at* http://www.nyu.edu/pages/lawreview/74/2/benkler.pdf.

[11] *E.g.*, BONNIE S. MCDOUGALL, LOVE-LETTERS AND PRIVACY IN MODERN CHINA: THE INTIMATE LIVES OF LU XUN AND XU GUANGPING (2002).

[12] *See* Swire, *supra*, note 4.

[13] *See* Gregory Shaffer, *Globalization and Social Protection: The Impact Of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1 (2000).

[14] BARRY E. CARTER ET AL., INTERNATIONAL LAW 687 (4th ed. 2003).

[15] *See* 5 U.S.C. § 552(a) (2004).

[16] Jon Swartz & Byron Acohido, *EU Scrutinizes Microsoft's Passport*, USA TODAY, June 12, 2002, at B3, *available at* 2002 WL 4727788.
[17] *See* ARTICLE 29 Data Protection Working Party, Working Document on On-line Authentication Services, adopted Jan. 29, 2003, 10054/03/EN WP 68, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp68_en.pdf.
[18] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 [hereinafter European Directive].
[19] *See* Press Release, The Court of Justice of the European Communities, Judgment of the Court in Case C-101/01 Bodil Lindqvist (Nov. 6, 2003) *available at* http://www.curia.eu.int/en/actu/communiques/cp03/aff/cp0396en.htm.
[20] European Directive, art. 6 1.(c).
[21] *Id.*, art. 8. Such special data may not be shared absent "explicit" consent, *id.* art. 8 2.(a), which is understood to mean an "opt-in" scheme.
[22] European Directive, Article 4, provides:

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
[23] Working Paper, Privacy on the Internet—An Integrated EU Approach to On-line Data Protection 5063/00/EN/FINAL WP 37, at 28 (Article 29 Data Protection Working Party eds., 2000) (applying the substantive law of a Member State under Article 4 in the context of cookies on hard drives in a Member State), *available at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp37en.pdf; *cf.* Swire, *supra* note 4.
[24] *See* ARTICLE 29, *supra* note 17..
[25] Lisa Jucca & Tom Miles, *Microsoft Fixes Passport to Meet EU Privacy Rules*, GLOBE & MAIL, Jan, 31, 2003, at B5.
[26] Matt Loney, *Microsoft Agrees to Passport Changes*, CNET NEWS, Jan. 30, 2003, *at* http://news.com.com/2100-1001-982790.html.
[27] Steve Stanek, Business Risks of Spam, Protiviti KnowledgeLeader, at http://www.protiviti.com/knowledge/current_feature/071103.html.
[28] Matt Hines, First Complaint Filed Under Can-Spam, CNET NEWS, Apr. 29, 2004, *at* http://news.com.com/2100-7349_3-5201906.html?tag=nefd.lede.
[29] *See* CAN-SPAM Act of 2003 § 5(a)(3).

[30] Eugene Kontorovich, A Positive Theory of Universal Jurisdiction, 80 Notre Dame Law Review 33-34 (forthcoming Nov. 2004).

[31] *See, e.g.*, Scott Charney, *Trustworthy Computing 2003 Year in Review*, MICROSOFT.COM, Jan. 23, 2004, *at* http://www.microsoft.com/mscorp/twc/yearinreview03.mspx.

[32] Article 25 of the European Directive states:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

[33] Trade Act of 1974 § 301, 19 U.S.C. § 2411 (2004).

[34] Commission Decision 2000/520/EC of July 26, 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce,-2000 O.J. (L 215) 7, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_215/l_21520000825en00070047.pdf.

[35] Joel Reidenberg, Testimony before the Subcommittee on Commerce, Trade and Consumer Protection, Committee on Energy and Commerce, U.S. House of Representatives, Hearing on the EU Data Protection Directive: Implications for the U.S. Privacy Debate (Mar. 8, 2001), *available at* http://reidenberg.home.sprynet.com/Reidenberg_Testimony_03-08-01.htm#_ftn23.