ELECTRONIC BANKING LAW AND COMMERCE REPORT

CONTENTS

APRIL 2001 | Volume 5 Number 10

Peter Swire on Privacy, Pay Phones, and Strong Crypto

by EBLCR

The law of cyberspace is the domain of Peter P. Swire, Professor of Law at the Ohio State University College of Law. From March 1999 to January 2001, he served as the country's first Chief Counselor for Privacy, responsible for coordinating administration policy on public and private sector uses of personal information. From his position in the Executive Office of the President, he advised the Clinton Administration on a broad range of issues, including financial services privacy, medical privacy, Internet privacy, transborder data flows, and encryption, and served as point of contact with privacy and data protection officials in other countries. Professor Swire, along with Robert Litan, wrote *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, published by Brookings Institution Press in 1998. He will be teaching at the George Washington University Law School for 2001-02. The *EBLCR* spoke with Professor Swire on March 20, 2001.

EBLCR *Last year the American Bar Association issued an interesting report by the Global Cyberspace Jurisdiction Project. How do you anticipate that issues of "cyber-jurisdiction" will ultimately be resolved?*

Swire There's this big debate between [regulating by] country of origin and country of destination—neither answer is very satisfactory. … One promising way out of that is to create some new institutions that have a basic core of consumer protection built in, whether it's through the payment system, such as credit cards, or intermediaries like eBay or Yahoo!, or new kinds of assurance institutions like BBB*OnLine*. I think we should be looking for a practical, workable way for companies to know

(continued on page 3)

Interview with Professor Peter Swire

(continued from page 1)

the rules of the road and for consumers to get a basic code of reasonable commercial practice.

EBLCR *Will the driver be market forces or government regulation?*

Swire In the U.S. a lot of it will happen from market forces. But in other countries that are less used to letting the market create those institutions, the governments will probably play a greater role.

I think the United States has been—and should continue to be—cautious about government-centered approaches to the Internet. The Europeans have more often thought that the government had to draft codes of conduct in advance in order to give consumers enough confidence to participate. The U.S. tends to trust more in early adopters on the company side, and on the consumer side to try things out until something starts to work.

EBLCR *It sounds like you're saying we just have to be comfortable with the situation being up in the air for a while. Is that right?*

Swire When you're talking about change—different providers, different business models, different delivery systems—all of this takes time. In the book I wrote with Bob Litan for Brookings [*None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*], we talked about the history of digital signatures. There were some early laws that tried to set up elaborate legal structures for digital certificates—Germany and the State of Utah were prime examples. Very capable people who tried to draft the law in advance turned out to draft laws that have hardly been used at all because they didn't really know what would work in the market. A better approach in many instances is to allow experimentation and address real harms, but don't try to figure everything out in advance. It won't work.

As with other attempts to guide e-commerce, we should make sure that well intentioned regulations do not end up interfering with business models that provide value to consumers.

EBLCR *We hear regularly from financial institutions that data security is their greatest concern when it comes to online banking.*

Swire It better be. Very important.

EBLCR *Do you think that the technical solutions exist—to satisfy financial institutions, their regulators and their customers—to allow for the full array of financial services over the Internet?*

Swire Yes, but we'll have to learn by doing. There's a wonderful history of an earlier system for distributed payment and that's the history of the pay telephone. If you think about it, it's a very risky thing to have a box containing money in remote places like next to roads in the countryside. My understanding is that there was a lengthy history of learning how to make pay phones tamper-proof. Originally, a bullet or an electric shock could open up a pay phone. But over generations of effort, we got it so we can put money in pay phones and think that the crooks are not going to steal it. We'll probably have to go through similar iterations before we really have security for the Internet. We'll try things. They'll be pretty good. There'll be holes in the security. We'll patch them. And we hope to make progress over time. It will take a number of rounds of effort by companies to have systems in place that are as good as the systems they have for the offline world.

EBLCR *Would you apply this same model to the wireless environment?*

Swire Security is not a one-time fix. Security is coming up with enough procedures so that you can match the security to the risk. Banks have learned how to handle very risky situations in the physical world. I'm confident banks will find ways to handle risks in the online world, but it's probably going to take a number of rounds of effort. The same goes for wireless.

There's a consensus now that banks can use strong encryption and that makes

wireless much more achievable. If you didn't have strong encryption and you were trying to do financial transactions over wireless, it would be obviously and easily hackable. Wireless is another example of why you need strong crypto.

EBLCR *Given the federal government's ACES program, should the financial services industry be thinking about a single digital certificate that can be used universally for communications in both the government and private sectors?*

Swire One of the great mysteries is why digital certificates have not spread yet. I have pushed the National Academy of Sciences to do a study on how to do authentication and privacy in the electronic environment, and the first meeting of the blue chip panel was held [in mid-March]. I'm pleased to have that underway because we need to have both strong authentication and consumer confidence in privacy for electronic transactions. Until that's solved, I'm not sure we're going to see digital certificates spread.

Let me say some more about that. There are some models of digital certificates—and ACES may be one of them—that have weak properties for privacy. These models assume that the system administrators will know everything about all the users. There are other alternatives, including work in a book by Stefan Brands, from MIT Press, [Rethinking Public Key Infrastructure and Digital Certificates] and others that show ways to do digital certificates without giving so much power to the system owner.

EBLCR *You critiqued the EU Privacy Directive in your book,* None of Your Business. *Why have so few companies signed up for the U.S.-EU Safe Harbor?*

Swire In talking to industry, one important reason that we don't have more companies signing up for Safe Harbor is that it turns out to be pretty strict. And so far, companies don't think that enforcement in Europe is very likely. So they don't see yet a strong incentive to sign up. If Europeans bring enforcement action, then there will be more company interest in Safe Harbor.

EBLCR *Do you think the EU would actually use its sanctions to shut down data flows to the U.S. in the future?*

Swire I think that in the right fact situation they would find it easy to do so. If there's some intentional violation of the privacy rule. But a general shut down of data flows will not happen. It would be more of a case-by-case situation.

EBLCR *In the event of a specific data flow shut down, what should the U.S. government do?*

Swire Well, the more it looks like the Europeans treating a European company and European data under European law, the stronger their case will be. If they're doing it in a non-discriminatory way, then they're basically enforcing domestic law. If they single out American companies, then it looks more like a case for the WTO. In my book, we discuss in detail how the WTO would apply if the Europeans discriminated against U.S.-based companies.

EBLCR *What about the contract model as an alternative to the Safe Harbor?*

Swire Contracts work for some companies, but you have to get the approval of each national authority. That will work better for the biggest companies that already have a presence in Europe. They won't work so well for small- and medium-sized enterprises.

EBLCR *How do you think the current debate over treatment of the financial services industry for purposes of the EU data protection directive will be resolved?*

Swire That's hard to say. Probably the new administration, at some point, will give a signal about its view about Safe Harbor generally and financial services will be part of that. The Bush Administration has not yet named any privacy officials and has not yet indicated what senior officials will work on privacy issues. Until we know about Safe Harbor in general, it's hard to guess what will happen with financial services.

EBLCR *What is the likelihood that the EU would decide Gramm-Leach-Bliley is acceptable*

under the Directive once they've seen it in place for awhile?

Swire Last year there was no way that I saw where they would say that Gramm-Leach-Bliley by itself was adequate. But times change, new administrations come to power, and they make new decisions.

EBLCR *What do you do about the privacy of data sent to countries like China, which have very different systems of government?*

Swire That's similar to asking about intellectual property in China. There are countries with less developed legal regimes for foreign investment and intellectual property and other parts of modern commerce. We wouldn't expect those countries necessarily to take the lead on privacy. Then you hope that global companies will hold themselves to the global standards and not use operations in a less developed country as a data haven.

EBLCR *Let's get back to the U.S. Based on your perspective as former Chief Privacy Counselor, can you offer any general comments on how the financial services industry has handled privacy issues to date?*

Swire I think the American Bankers Association and other trade groups have done some promising things, including education, in the privacy area. And the industry has a very strong history of confidentiality.

The hard thing for the banking industry is how to figure out ways to be state of the art marketers and also maintain their tradition of confidentiality. And different parts of the financial services company have different instincts. So, some of the "go-go" practices really violate people's sense of what's appropriate. Sometimes when senior managers learn about the practices three or four levels down they're surprised and maybe not that happy with what some of their own people are doing. The *U.S. Bancorp* case was a big surprise to many industry people. I think a lot of them didn't realize what practices were actually happening—even in some of the large and well-run companies.

EBLCR *U.S. Bancorp is an example of a company that decided to respond by trying to tighten up their privacy regime and establishing a new position as chief privacy officer. What do you think about that trend?*

Swire I think it's a good trend. I was basically the Chief Privacy Officer for the U.S. government for two years. I think I was able to help decision makers meet their legitimate goals and do it in a way that was consistent with privacy. By anticipating problems and coming up with better data practices I think you're helping the organization and still achieving the organization's goals.

EBLCR *What about the benefits of information sharing?*

Swire In our book we talked at length about the benefits of information flow because we felt that some of the European regulators did not appreciate that enough.

To the extent that we live in a free society, how much will individuals have a say in how their data is used? My preference is to make sure that customers have a choice. One of my biggest concerns under Gramm-Leach-Bliley is that it allows a credit card company or a bank to use the checking account information and ship it directly to affiliates who are travel agents or health insurance underwriters. That kind of affiliate transfer to operations that are *very* different from the basic business transaction I think is surprising to people, and I think people should have some say. Whether that has to be in law I won't even say, but I think good business practice would be to do what's reasonable and expected by people, but not to use information in ways that would really surprise the conscience of people.

EBLCR *Do you think that the industry could do a better job of letting people know how they do benefit from information sharing?*

Swire Well, I think the political debate is under way now. There are major studies funded by industry that were recently released to highlight the benefits of information sharing. There are very valid reasons to share information—for law enforcement

purposes, to prevent fraud, to make credit more freely available, for example. The question for me is how do you do the legitimate sharing of information and stop the illegitimate sharing? The debate should mature some more and not be between an absolute right of privacy and the slogan that information should be free under all circumstances. The companies that say that information should be free in the privacy debate never say that when they're in the intellectual property debate.

EBLCR *What do you feel were the most important accomplishments of the Clinton Administration with regard to consumer privacy?*

Swire Until recently I clearly would have said the [HIPAA] medical privacy rule. But now it may be in the process of being repealed and I think that's a political and a substantive mistake. [Ed. note: After the interview was completed, the Bush Administration decided to permit the medical privacy rule, as issued last year, to go into effect.] I think there's a consensus in the United States that people's medical records deserve confidential treatment and we went to great lengths in the final rules to respond to industry and other comments so that good uses of medical information were permitted and information that should stay confidential would stay confidential. To me, a disappointingly large fraction of the criticisms of the rule are simply inaccurate. The HealthPrivacy.org Web site [www.healthprivacy.org] has a myth and reality list about the medical privacy rule that quotes some of the criticisms and shows how they're not accurate.

EBLCR *Should the U.S. have a privacy office with regulatory powers, as they do in the EU and Canada? If so, what powers should that office have?*

Swire I believe it is helpful to have a policy office, in OMB or the White House, that's expert in privacy. That's important for the government's own use of data. It's also important for what's called the clearance function, as agencies come up with proposals, to make sure that data is being handled in similar ways across different agencies. What a White House office cannot do is be an enforcement agency. For that you need some office that enforces the law. To date there's been very modest funding for those offices. The exception may turn out to be the banks where they already have a staff of supervisors, but in most other areas we don't have regulatory staff that already exists.

EBLCR *How about the FTC?*

Swire The FTC does a very high quality of work. They also historically have very modest staffing. The question is whether there can be enough of an enforcement structure to be credible, otherwise it could be a very hollow regime.

That's one reason why I think that third party groups, like TRUSTe or BBB*OnLine*, are so important. They have the potential to scale in ways that federal agencies do not. That's basically what happened with financial accounting in the 1930s. Consumers needed to have confidence in some thing that was hard to measure—the financial solvency of companies—and the accounting firms filled that gap…You trust CPAs; you trust CPA audits. In a data society it's not surprising that we're going to need good audits for data practices. But we have to create those institutions, just like we have to create the business models.

EBLCR *State legislatures have been active on privacy issues and many fear a potential privacy law patchwork. Will there be federal privacy guidelines that preempt state law?*

Swire I think that the possibility of state laws is clearly the biggest reason to eventually expect federal privacy law. Without the threat of state laws, industry would have no reason to ever tolerate federal privacy laws and so this dynamic between the states and the federal government is going to be really the key thing to watch, to try to predict the next five years or so.

EBLCR *Is there anything else you'd like to address?*

Swire Let me talk just a little bit more about the medical privacy rule. A lot of health organizations are part of holding compa-

nies, so what happens to HIPAA will matter a lot to the financial services industry. If the medical rules go into effect, then even more than Gramm-Leach-Bliley, that will lead many organizations to institutionalize privacy inside their companies. So it would be a very big deal if the HIPAA rules go into effect.

If the HIPAA rules do *not* go into effect, then it provides privacy supporters with a very powerful argument for the need for change, because then we would have no medical protections and no Internet protections. Then at both the state level and the federal level you'd have two hot button issues pushing privacy forward. Because there's such a broad consensus that medical records should be protected, I think it's shortsighted of some industry actors to think that killing those regulations will help in the long run. There's a real chance that it would go the other direction and further show the political system that regulation has to be put in by legislators. Let me just leave it at that. ■

Outsourcing Rewards (Usually) Outweigh the Risks

by Erika Crandall

In order to retain customers, gain market share, and develop valuable industry recognition, financial institutions are being driven to deliver technical solutions—often Internet-based—at a record pace. This has led to the increased usage of outsourcing arrangements with third-party vendors. These vendors may be marketing unproven solutions or may be financially unstable, operating in a distressed environment in which expenses surpass profits. Because of the vendor's potential shortcomings, a financial institution could expose itself to high levels of risk. In light of these possibilities, financial institutions need to continually review their risk tolerance levels and the financial viability of vendors with whom they do business. The financial institution can then determine whether the potential risks of outsourced arrangements are at a level that the institution believes is appropriate.

Despite the risks of outsourcing, partnering with a vendor often makes business sense. There are inherent benefits for a financial institution when a third party is responsible for the creation, maintenance and enhancements of an application. Outsourcing allows the financial institution to focus on its core competencies and divert fewer of its own internal human resources to offer its customers a new service. Moreover, an outsourced solution may be less expensive for the financial institution because the vendor absorbs and amortizes the research and development costs associated with the solution's creation and development.

The many potential rewards of outsourcing arrangements can, however, only be achieved if the financial institution takes a disciplined approach to vendor management. This article identifies potential rewards from a well-disciplined relationship with a third-party vendor, details the risks inherent to the relationship, and provides recommendations for managing third-party vendor risks in a thorough and rewarding manner.

First Things First: Developing a Business Case

In this fast-paced market, financial institutions are always on the lookout for new services and products in order to build a business case around the service. Not all of these new services can or should be developed in-house. Before committing to an option, the financial institution should thoroughly review the business case underlying the proposed project, documenting the benefits that the new service, product or process flow will provide. An in-depth business case provides the institution with the necessary framework to make an informed choice as to the type of solution required. Once an institution determines the need for a solution—for a new or improved product or service or for streamlining an internal process or production flow—it should thoroughly review the available solutions, which typically include:

Ms. Crandall is a Vice President at Wachovia Bank, N.A. and is based in Winston-Salem, N.C. She serves as the bank's eBusiness Policy Manager and chairs its Privacy Council and eRisk Assessment Committee. She can be reached at erika.crandall@wachovia.com.