

DIRECT

Bad Law Rising

By Ray Schultz | Jun 1, 2006 | 1375 words, 0 images

YOU THINK YOU HAVE it tough with privacy regulations? It could be worse.

For starters, you could live in Europe. Unlike in the United States, privacy laws there are based not on preventing harm, but on giving consumers control.

Or European ideas could seep into the U.S. market. And regulators in other fields could have a dampening effect on financial services marketing.

So says Martin Abrams, executive director of the Center for Information Policy Leadership at Hunton & Williams, Washington.

In a recent Q&A with Direct, Abrams provided an overview of the privacy challenges facing financial marketers. In general, he's wary of regulations that fail to enhance "either operational efficiency or consumer protection."

But he says such regs could be in the offing just the same.

DIRECT: What can financial services marketers expect on the privacy front?

ABRAMS: Privacy law in the United States is unstable. And it's unstable because of the way we've built it, and the way business processes have been globalized over the last six to seven years.

DIRECT: That sounds ominous. Can you elaborate?

ABRAMS: There are three reasons for the instability. The first is that privacy law in the United States was based on identifying and addressing a harm. It started with the Fair Credit Reporting Act. The potential harm was that inaccurate information could be used to make important decisions about individuals when they apply for credit, and that this could be misused in other settings if it were not regulated. The FCRA was followed by numerous other privacy laws, one layered upon the other. Probably the most important one other than the FCRA itself is the Gramm-Leach-Bliley Act. The perceived harm was the sharing of information with other organizations without the consumer having a choice. On the security front, it also specifies that organizations need to safeguard the data in an adequate fashion.

DIRECT: How does this harms-based approach differ from the European model?

ABRAMS: The European model begins with the concept of people having individual control over the information that

pertains to them. It's a controlled-based system, rather than a harms-based system.

DIRECT: Is our system working?

ABRAMS: We've put lots of dollars into enforcement through the FTC or the various bank regulatory agencies. Our enforcement in the United States is really the envy of the rest of the world.

DIRECT: So what's wrong with our approach?

ABRAMS: This way of building law upon law has inevitably created conflicting requirements.

DIRECT: What are the other reasons for the instability?

ABRAMS: The second reason is that a lot of privacy law is based on decisions by the Federal Trade Commission. The FTC does not regulate depository institutions, but it's taken actions to define deceptive and unfair practices, and these influence the way any new law is considered by Congress and the state legislatures. They even affect the way financial services companies are regulated.

DIRECT: How could regulation of other industries affect financial services?

ABRAMS: On a strategic level, we could begin to see things like a push to oversee the unregulated parts of the economy. Let's say you work at a financial services company and you notice that retailers are required to have base-level information security in place to protect the integrity of the payment system. You might say, "Great." But what if those requirements are more robust than those in Gramm-Leach-Bliley? Is that a stable place to be?

DIRECT: And on the tactical level?

ABRAMS: We incrementally require change through the regulatory process, especially in the area of information security, but not always in a way that enhances operational efficiency or consumer protection.

DIRECT: For example?

ABRAMS: It comes into play with the authentication requirements in the financial services arena (to protect consumers from identity theft). The regulations are very granular in discussing what they mean by two-factor authentication.

DIRECT: Can you define two-factor authentication?

ABRAMS: It means I combine a password I've given you with a fact only you would know.

DIRECT: Like my mother's maiden name?

ABRAMS: Yes. But it's always very dangerous when regulators begin to describe how something like two-factor authentication will work. Technology changes the best way to do these things over time. But then the fraudsters pick up on the way the systems work and re-engineer them for their own benefit.

DIRECT: And the third factor in creating instability?

ABRAMS: The third reason is that the nature of data transfers has changed because of the way we've globalized business processes post-Y2K. It started when we began to build common data-application modules. We've managed these or outsourced them to other organizations to supervise. This means more of our regular business processes that use personal information are being managed in other locales. It's hard for those outside the United States to apply global data transfer to a system of laws that's layered the way our system is. So there's sort of an inherent sense that U.S. privacy law is unstable.

DIRECT: Will we be moving to the European model?

ABRAMS: There's a growing pressure to have an information policy system in the United States that better links with the rest of the world. Now, that doesn't mean transferring European data protection to the United States; it probably means a new and different privacy structure. But that's not going to happen until there's a leadership push from the top, and that's probably three to five to seven years away.

DIRECT: What's the risk in that?

ABRAMS: Other economies use information. But the United States is unique as a marketing economy because of the way we prospect. Any changes in privacy law have to be respectful of the incredible value that this marketing approach has created for U.S. consumers.

DIRECT: We see what you mean by instability.

ABRAMS: There's also one other potential shock to the system, and it's almost an unavoidable one. It's that privacy notices are getting to be more clinical and easier to read. The financial services regulators just completed research on a prototype financial services privacy notice. Since Gramm-Leach-Bliley focuses on data sharing, the notice focuses on data sharing. It lists the seven types of sharing that can take place in a financial company, and where a consumer does and doesn't have a choice. Financial services regulators say they've been asked by consumers: 'How can you give us a sense the data is being protected when it's being shared so robustly?' That regulatory process has another two years to run, but as those notices get more clinical, the educational challenges will become even more critical.

DIRECT: Will this cover both offline and online media?

ABRAMS: All media.

DIRECT: What would you advise financial companies to do at this point?

ABRAMS: To understand that their use of information is going to become more transparent over time, and that they must convince consumers that more robust data flows are in their best interest.

DIRECT: Is that something you do as an industry, individually with your customers?

ABRAMS: You need to do both. But industry trade associations tend to react more slowly than do individual participants in the marketplace. Companies lead the way.