SELF REGULATION OR PRIVACY LEGISLATION

Dale Skivington – Former Chief Privacy Officer, Eastman Kodak

We just heard a great overview of what's happening at the State and Federal level to regulate privacy. What I'm going to do is talk about what's going on internationally and then circle back to the United States, because what's really fascinating is a lot of what's happening in the U.S. is driven by what's happened outside the U.S.

In 1999, I was on an assignment for Kodak in Europe. I was working on an acquisition and spent three months there. During that time I had an opportunity to read the local newspapers and talk to local law firms about the European Union's new Social Compact. There were laws that were going to be developed Pan-Europe to regulate certain issues relating to employees and customers. I thought I'd see laws relating to discrimination—age, gender, race and other kinds of wage legislation. However, the thing everybody was talking about in Europe was privacy regulation. The E.U. Directive on Data Privacy, which had been enacted, was going to be implemented around 2000. The Nation States had to implement their regime over a specified period of time.

Essentially, the Directive provided that European companies were not going to be permitted to transfer personal data (and it defined personal data very broadly, i.e., name alone) to any place outside of Europe if the country didn't have "adequate privacy protection". The US approach to privacy was sectoral (we had privacy legislation that was related to specific types of information such as health information, financial information). It wasn't omnibus as it didn't cover all personal information. Thus, the EU didn't consider the United States to have adequate protection. The press was reporting that as soon as this Directive was effective, companies were not going to be able to transport data out of Europe into the United States, or elsewhere for that matter.

When I came back from that assignment, I met with a team of senior people at Kodak and indicated that this was really going to have major implications for companies and it could preclude transfer of data outside of Europe. We had just integrated our operations worldwide and we had implemented SAP software to allow us to be more transparent as to where our employees were located. We had just began to launch Kodak.com, which was our internet offering, and we were implementing that worldwide to sell our products and services. Servers were located in places where the European Union was not considered to have adequate protection.

When I spoke with the General Counsel and some of the executives about it the issue they wanted to understand was what solutions existed. The answer seemed to be in policy deployment. The U.S. was negotiating with Europe for the Safe Harbor Accords, which provided if a company committed to policies to protect personal information, that data would be allowed to be transferred provided the Company sign up to the Safe Harbor principles, which in turn provided the FTC could enforce if the company violated the policies.

Kodak was one of the first companies to enter into the Safe Harbor, but in order to do that it took a lot of work to determine where data was, where it was transferred, what kind of notice, choice, access and security and auditing was being done. What the Safe Harbor Principles did was incorporate what the FTC had already stated were fair information practices. So Kodak was among several other companies which decided to appoint a Chief Privacy Officer to lead these policy changes and initiatives, and I was fortunate enough to be assigned that role.

Today there are over 2,500 certified privacy professionals. But at the time, we were in a back room with a professor from Columbia University. There were about five of us. We were brainstorming and debating what does a good privacy policy look like and what would the FTC expect? We decided to actually meet with the FTC and get their input. This was during the Clinton administration. They understood that the emerging business of e-commerce was important to the revenues of the US and they didn't want to disadvantage companies from being able to participate in the global economy. The FTC helped us understand what it is they expected from the perspective of compliance with the Fair Information Practices.

We then focused on what our customers were telling us was of

concern to them. When you're a company with a strong brand you don't need regulations to tell you what to do. If your customers are not happy then you've lost the battle. So for me, being Chief Privacy Officer at Kodak was a dream because I had great support from the Company. The Chief Marketing Officer, the CFO, and Director of HR were concerned about how the use of data would be perceived.

We also participated in an organization called Privacy Leadership Initiative. It was a group of brand companies which came together to consider looking at what consumers really wanted and needed related to use of data on the internet. We decided to focus on transparency. We kicked off what we called the Notice Project. The Notice Project was intended to solve the problem of complicated notices required under GLB and HIPAA. We took a look at what the food industry had done on food labeling, because everybody who has been on a diet knows where those labels are and knows how to read them. We worked with a very broad based coalition. We had international participation because once we suggested a standard we wanted buy-in from the regulators in Europe and Asia.

Asia was really interested in the issue. Why was that? Because of all the data that was going in and through to Asia. India was becoming a powerhouse of industries collecting personal data of U.S. citizens, and they wanted to be sure that they were seen as a place where data could be safe. They were considering regulation. We worked with an organization of Pacific companies and regulators. We also worked with consumer advocates from Europe, Asia and the US. We also engaged representatives from the health care sector and the financial sector because they already had a pretty comprehensive notice regime and it was important for our proposal to be consistent with their regulatory scheme. That was probably one of the most difficult things to accomplish.

But we did come up with what we thought was a good notice proposal. I spoke at a conference in Sydney, Australia where we introduced it to the privacy commissioners worldwide, and it was well received. I have a copy of the notices that we developed and Kodak's implementation of it. I was going to pass it out but I actually decided what I'd really prefer you to do is go onto www.kodak.com, take a look at our privacy notice, and while you're there, buy a few Christmas presents.

Thereafter we worked with legislators on how our model notice

might fit within the legislative proposals. We argued that clear notices were a big part of the solution. However, there were a few large data breaches which started a swirl of Congressional activity.

Just to give you a little insight into the difficulty of writing omnibus federal privacy legislation: let's assume you want to try to legislate providing notices when you collect personal data. What does "personal data" mean? In Europe, as I told you, it means name alone, an IP address. What kind of information requires notice before collection, business information? In Europe, if you collect and share somebody's business address, the privacy regulations apply to that data. So you can see just defining what is personal data is difficult for Congress in terms of not making it so burdensome that entrepreneurial companies will just stop collecting data altogether and we won't have the kind of innovations we need and to allow our economy to grow.

What type of notice do you need to give? Do you need to give notice about everyone with whom you share personal data? California law says yes, you do. However, what about when you buy something online and the company gives your address to UPS to ship it to you. Is that the kind of notice you want? That your data was sent to UPS? You can imagine what these notices would have to look like. Is the consumer more interested in such notice, or holding companies accountable if they give data to another who doesn't have the same level of security and commitment to keeping that data private?

Choice is another part of this legislation that is difficult to get right. Is it opt-in? Is it opt-out? Some would argue it should always be opt-in, I always want to click. But when you talk to consumers about companies they trust and whom they do business with, the last thing they want to do is have to be bothered with clicking multiple times every time they buy something from the trusted site.

The most difficult part of notices is how do we explain to consumers about cookies and other technology that aggregates data. That was what the Sears case was about. What happened in the Sears case was they put a notice indicating they were "looking at what you ordered, what you looked at and also what you looked at on other people's sites." They were aggregating all of that information and then sending out specific advertisements for products that the consumer might be interested in.

The FTC, however, found fault with the notice since they didn't

think that the notice was clear enough. They brought a proceeding against Sears. In the past, the FTC would not have brought this case because the FTC's position was harm's-based. They would bring enforcement activity when a consumer was harmed by the use of their data not just for poor notices. This case did not result in harm from a financial perspective. David Vladeck—the Privacy Czar at the FTC said he's going to use a new standard for deciding whether there is harm, and that is whether the "consumers' dignity has been offended."

That has caused the privacy community a lot of concern because that is a very different approach. Actually, for the CPO's of the world, it makes their role even more critical because they need to kind of be the conscience of the organization and determine what offends dignity in terms of the way you're collecting data and how you're describing it. Also, as a result of this standard, companies may be more inclined to see privacy legislation passed that is a harm-based statute. Legislation might also be able to fix some of the issues that we were talking about earlier, the difficulty of dealing with many different state breach statutes by having it be preemptive. Although I doubt privacy will get much attention this session, I expect we may see some legislative proposals to consider. I do expect there to be a continued interest in enacting Federal privacy Legislation.