NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 5, ISSUE 2: SPRING 2004

Reflections on the NC JOLT Symposium:[1] The Privacy Self-Regulation Race to the Bottom

Chris Jay Hoofnagle[2]

It is 1904. A raging debate is taking place between consumer advocates and manufacturers of foods and drugs.[3] Manufacturers were profiting from the sale of adulterated and mislabeled products, and, in particular, through the marketing of sometimes dangerous "patent medicines." Industry self-regulation resulted in a race to the bottom, where adulteration of food in order to increase yield was common. Honest companies could not compete with those who could cut costs by adulterating or misrepresenting the contents of food. This Wild West of food and drug safety sparked calls in support of a federal law requiring food and drugs to be safe and pure. Manufacturers opposed such legislation, arguing that self-regulation would produce safe and pure products; that federal legislation is paternalistic, as it controls interactions between buyers and sellers; that it would harm innovation; and that it would interfere with free enterprise rights.

We are in the Wild West of privacy and security today. As was the case with consumers of food and drugs one hundred years ago, today's consumers know little about the actual practices of companies that have their personal information. There is skyrocketing identity theft, stalking made possible through the sale of personal information, and a shift in power from individuals to

---

[1] Hosted by the North Carolina Journal of Law & Technology, University of North Carolina, Sept. 26, 2003.

[2] Chris Jay Hoofnagle is Associate Director of the Electronic Privacy Information Center. He is the author of *Protecting the Fundamental Student Right to Privacy*, CAMPUS PRIVACY REV. (forthcoming 2004); *The EFOIA Amendments of 1996*; and *Consumer Privacy in the E-Commerce Marketplace 2002*. He has testified before Congress on privacy and Social Security Numbers, identity theft, and the Fair Credit Reporting Act, and before the Judicial Conference of the U.S. on public records and privacy.

[3] PHILIP J. HILTS, PROTECTING AMERICA'S HEALTH: THE FDA, BUSINESS, AND ONE HUNDRED YEARS OF REGULATION (2003).

business and government data collectors. There also are more subtle, cultural harms. Individuals feel more vulnerable to strangers and, as a result, are less likely to engage in social behaviors like exchanging phone numbers.[4] There is an emerging field of activism that argues direct marketing pollutes the "mental environment"[5] and that economists need to account for distraction as a harm or cost caused by privacy-invasive advertising.[6]

Consumer advocates have called for broad ranging privacy protections—ones that not only require accurate notice but also place a ban on certain uses of personal information. The industry, perhaps best represented at the North Carolina Journal of Law and Technology Symposium by Chris Mustain of IBM, counters these calls with the same language and arguments used to avoid accountability in the food and drug debate—that privacy law will infringe upon innovation and free enterprise rights.

With the hindsight of nearly one hundred years of food and drug regulation, we now know that the manufacturers' arguments against safety and purity laws were specious. Self-regulation encouraged fraudulent and unpalatable practices. Philip J. Hilts, in his recent book *Protecting America's Health*, illustrates some well-documented examples: companies bottled ordinary tap water, colored with dye, as cancer cures. Others marketed miracle medicines for children, which were in fact opium. Deception was common in food packaging—for instance, real honeycombs would be combined with laboratory-created glucose to create "natural honey." The advertising industry, which was growing in power from revenues made through marketing patent medicines, masked

---

[4] May Wong, *Online Data Conflict With Desire for Privacy*, WASH. POST, Dec. 26, 2003, at A15, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A30795-2003Dec25 (on file with the North Carolina Journal of Law & Technology).

[5] Kalle Lasn, *The Birth of Mental Environmentalism*, ADBUSTERS MAG., Nov.-Dec. 2001, *available at* http://www.adbusters.org/magazine/38/mentalenvironment (on file with the North Carolina Journal of Law & Technology).

[6] Carrie McLaren, *Attention Economics*, STAYFREE! MAG., Summer 1999, *available at* http://www.stayfreemagazine.org/archives/16/intro.html (on file with the North Carolina Journal of Law & Technology).

these bad practices.[7] Manufacturers not only opposed purity and safety laws, they even opposed laws that required companies to give notice of ingredients within their products. As a result, instead of having a basic standard of product safety, individuals were supposed to evaluate product integrity based on brand reputation and the representations of ad men.

Laissez-faire approaches did not work for food safety, a field in which there are significant economic incentives to provide quality products. However, regulation in that field did have an unforeseen, positive impact. Regulation made modern pharmaceutical science possible and has led to a system that, although imperfect, creates incentives for the creation of safe and effective drugs.

I think we will eventually come to a consensus that self-regulation will fail to protect privacy for the same reasons that it failed to ensure quality food and drugs. Self-regulation shields companies from accountability and encourages a race to the bottom. It gives little incentive to design products with privacy in mind.

Unlike the food and drug industry, it is impossible for individuals to tell what actual information practices are employed by companies. Food and drugs can always be tested for adulteration. Suspicious chemicals can be analyzed for toxicity. The same is not true of privacy. Privacy-invasive practices are opaque and kept that way deliberately. Today, our primary window into actual practices is the privacy "notice," which is filled with puffery and vague language. These notices proclaim that companies "care" about our privacy and only "share" information with "trusted third parties" and their "corporate families." When practices are removed from the fog of advertising and public relations, however, we find that some major companies have a strange definition of "care" and "trust." The company that says "we care about your privacy" but sells your phone and credit card

---

[7] *See, e.g.*, Inger L. Stole, *Consumer Protection in the Historical Perspective: The Five-Year Battle Over Federal Regulation of Advertising, 1933–1938*, 3 MASS COMM. AND SOC'Y 351–72 (2000).

number to telemarketers[8] is not much different from the huckster who collects discarded horses in Manhattan for sale as "beef" in New Jersey.[9] Both examples are real, and if they represent "innovation," perhaps their definition of the term is just as strange as these companies' understanding of care or trust.

Like consumers in the quest for pure foods and drugs, the privacy community will have to document harms and continue to put pressure on policymakers to make progress. It is likely to be a long quest—after all, regulation of food and drugs still is not perfect, and new challenges are constantly presented in that field.

I hope that in the privacy debate we can foster a more nuanced understanding of whether regulation creates or hinders freedom. In food and drug law, regulation created great freedoms for individuals. Individuals have the freedom to purchase any food or other product without assuming unreasonable risks. It also created one of the most profitable industries in the United States.

Similarly, we could look to a future where privacy and security are designed into products, one where the landscape or architecture of data collection respects the individual and only requires personal information when necessary. Privacy and security should be as natural as safety and purity. Just imagine wireless phones with built-in end-to-end encryption that prevent interception of your conversations, accompanied by legal rules that prevent the phone company from selling the digits you dial to direct marketers. Imagine anonymous payment systems, where customers can shop with the confidence that their data cannot be provided to spammers or to government agents interested in the books, music, or web sites visited. Imagine more secure credit granting systems, ones where individuals can lock down their files so that impostors cannot obtain credit in their name.

---

[8] State Attorneys General have initiated a number of cases to address "preacquired account telemarketing"—the selling of customer account information to telemarketers. Capital One, Chase Manhattan, Citibank, First U.S.A., Fleet Mortgage, GE Capital, MBNA America, and U.S. Bancorp all have provided their customers' personal and confidential information to fraudulent telemarketers. *See* Chris Jay Hoofnagle & Kerry E. Smith, *Debunking the Commercial Profilers' Claims*, PRIVACY J., Aug. 2003.

[9] HILTS, *supra* note 3, at 57.

One thing is for sure—these products will not create themselves. Only a framework of rights and responsibilities for data will create the environment necessary for their development. "Fair Information Practices" is the framework traditionally proposed by privacy advocates.[10] Such practices require companies and governments to minimize the amount of information collected about individuals. The presence of personal information in databases must be disclosed. When data is collected, it must be accurate, complete, and up-to-date. Data collectors must be legally responsible for information practices. Information must only be used for purposes consistent with its collection. Personal information must be securely handled. Finally, individuals must be able to access and correct their data.

One could look at these set of requirements and say that they are paternalistic and infringe upon enterprise rights. One could also see great freedoms—freedoms from unwarranted government intrusion, freedom from intrusive advertising, and a future that provides basic respect for the individual.

[10] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy: (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1 (2001).