

---

---

EDITORIAL POSTLUDE

---

---

HERBERT JACK ROTFELD

---

---

Privacy Crimes, Annoyances and  
Self-Defeating Business Practices

---

**It appears that everyone says they want privacy, but no one wants to be left alone. Every journal article on the topic presents additional conflicts and contradictions of what people say they want, what the consumer advocates say is needed, and the self-inflicted harm consumers create. At the same time, business practices undertaken by managers recruited from the shallow end of the intellectual gene pool extend from trivial privacy invasions to the facilitation of cyber crimes. Unfortunately, the consumer protection debate has combined the annoying with the criminal, to the detriment of public policy planning that should focus on the latter.**

---

University faculty are required to place detailed statements of course requirements, work expectations and the basis for grading in the course syllabi. Campus administrators treat these documents as akin to legal contracts and this information is commonly placed online, along with other important study materials. Yet, college instructors report that within days of the final exam, many members of the class do not know important information that the syllabus spells out in mind-numbing detail, such as what the final exam would cover, the date of the test, or how to calculate their final grades. After four months, grade-conscious young people exhibit an almost studied ignorance of the guiding documents of the class, just as these computer-familiar tech-savvy students have not accessed recommended cross-links of study questions, sample cases, or other online course details.

Modern college students come to campus with a greater computer familiarity than those of any prior generation, or so we are often told, although a significant number of them often seem unwilling to use computers beyond e-mail to maximize the experience for which they (or their parents) pay many thousands of dollars. Computers can help

students prevent grading difficulties, and the majority knows how to do that, but the puzzle is those who don't.

Similarly, numerous privacy-desiring computer-literate people operate in a seemingly ignorant state, unaware of the various marketplace rules that could protect their privacy (Turow 2008). People sometimes read warnings, mostly not. Sometimes they are cautious, other times careless. Some people, sometimes, can be educated to attend to certain details (e.g., see: Rifon, LaRose and Choi 2005; LaRose and Rifon 2007; Nehf 2007), at least in a short-run context as illustrated by research. The broader and not-unexpected finding is that a number of factors come into play unrelated to actual knowledge of the electronic systems involved (e.g., see Nehf 2007; Pitt and Watson 2007; Youn 2008).

The simplistic explanation would be to assert general consumer illiteracy that logically would extend into any realm where people lack an interest to delve into the details of the subject matter (e.g., why people do not wish to understand financial information, Rotfeld 2008). Alternately, regardless of how familiar one might be with programs or machinery, privacy directives become so confusing, and often contradictory, that the simple consumer solution is to ignore the "newest" information by just making visceral decisions based on what emotionally feels correct (as was explained for health information, Rotfeld 2009). But these contradictions between what people say they want and what they do appear more basic, almost weirdly anomalous. Despite consumers' strong claims of privacy desired, their actual behaviors include activities that guarantee a lack of privacy, giving businesses or the world at large a view to their most personal information (e.g., see Norberg et al. 2007; Anonymous 2009).

The privacy literature in some ways sounds reminiscent of what a South Georgia county sheriff once jokingly noted as the types of problem drivers during the rare winter day when snow accumulated on the local roads. Local drivers could act entranced by the strange view of the mysterious white stuff coming from the sky, but the bigger problem is the northerners passing through who are probably yelling to passengers, "Hey, no problem," as if the roads were clear and dry. Similarly, the privacy-aware consumers boldly go forward thinking they can handle anything, while others behave with apparent ignorance as they are caught in data sweeps that send all sorts of unsolicited advertising messages or result in identity theft. The dichotomy might be a tad overly simplistic, but those caught in various privacy traps are not just small children and people who never turned on a desktop computer before the age of 55.

Both public policy decision making and the self-regulation concerns of honest businesses need research on how to maximize consumer

awareness of potential problems. Yet too many issues have become intertwined to the point where lines are not so clear as to exactly what is meant by privacy itself, and where consumer protection or public policy should focus. Details are important, because if you cannot say what you mean you can never mean what you say. It sometimes merely requires you to be specific. (This problem could also be applied to the regulatory problems dealing with the sometimes overly expansive pejorative terminology of predatory lending; e.g., see Delgadillo, Erickson and Piercy 2008).

Clearly, privacy protection reduces cybercrimes such as phishing, identity theft and criminal invasions of business' credit card data. As people seek new jobs in difficult economic times, online job listings provide another realm of consumer abuse. The increasingly popular social networks generate another avenue of potential problem, as people act exactly the opposite of self-professed claims of privacy desires, so not unexpectedly an estimated 13 percent of users experience some degree of privacy abuse. Cybercrime has become a major national security concern, so consumer education for self-protection in this area becomes especially crucial, though even experts can't easily recognize some new forms of phishing e-mail (Anonymous 2009).

As with many crimes, consumer awareness of dangers is a key, at least for discouraging the criminals if not fully preventing the crimes. Yet even here, at some point, people become casual or careless. Again, the human behavior parallels extend beyond electronic privacy. Despite the simple rules for travelers to discourage pickpockets, men walk through crowded airports with fat wallets visible in their back pants pocket known to criminals as "the sucker pocket" for the ease with which it can be removed. Women walk through downtown city streets with thin-strapped purses dangling behind their backs as if they are leaving bait for a quick purse grab.

Of course, these people are not stupid, ignorant or lazy. To some extent, privacy awareness is an ongoing effort, and it could prove draining as a constant awareness of even little details. The simple subconscious reaction is to get comfortable or casual, as some fears are perceived as overblown.

Consumer self-protection taken to the extreme would be akin to the medical office receptionist on the television program "Northern Exposure" who would not date anyone whose medical records indicated the slightest potential for a future health problem. Visiting the grandparents many years ago in Florida, my younger sister, her husband and I all decided to drive to a nearby beach just after sunrise. Even North Miami

Beach can have cool mornings in late December, so we did not stay long on the deserted sand. Telling our grandparents where we went, they were aghast. "You shouldn't go there. That's where they have all the illegal drug dealing." We said that it was not going on when we were there, as we had the beach to ourselves except for the brief period when we saw one man loping along the shoreline with his small dog. "The drug deals were there. You just didn't see them." Apparently that specific area was named in a past police report published in the local paper, and thus to our grandparents it became a place to avoid. And maybe the place should be avoided at certain times, but that morning the scene was serene.

Consumers' realistic fears can cross into paranoid. Fatalism or denigration of possible dangers proves not so irrational as people factor probability of harms versus desired freedoms. Full protection would require never opening e-mail from names not immediately recognized, never giving a credit card to a waiter, never shopping online, or maybe, never using a credit card or e-mail at all. Still, one can live within realistic cautions. There are dangers that can be controlled or cautions to be noted and practices to be aware of avoiding.

It becomes easier to belittle the dangers of cybercrime when the discussion readily combines it with the innocent or innocuous business uses of privacy data. The error would be to confuse the dangers of potential criminal abuses with privacy annoyances of spam or just being on too many mailing lists.

For example, many retail store chains have loyalty programs. Most consumers see these membership cards as mechanism for discounted prices, something that has been positively supported by columnists at consumer protection web sites or in *Consumer Reports*. It is intuitively logical that these same consumers probably recognize that these loyalty programs enable the tracking of purchases tied to personal addresses or phone numbers that could be sold to third parties, but they don't care. In theory, the marketing messages are better targeted to the consumer interests, while a company that abuses the card program with invasive telemarketing or sales of customer lists to offensive product distributors could discourage both existing and potential new customers. But at worst, it can be an annoying nuisance.

The strong popularity of privacy as a research topic stems more from consumer fears of privacy invasions than the criminal problems that need to be controlled. Sometimes, studies of privacy literacy start from the researchers' presumptions of what people should know instead of the pragmatic realities of what consumers want to know or potential intrusions they might wish to prevent. Privacy literacy therefore goes

beyond not only knowing how to keep information personal when it is desired to do so, but also knowing that many other times the dangers of crime are minimal and the risk level acceptable (e.g., see Norberg, Horne and Horne 2007).

The apparent contradictions between what consumers say and what they do might not all be contradictory. The understanding of technology includes knowledge that not all privacy intrusions are invasive, thus, not all are invasions.

## REFERENCES

- Anonymous. 2009. Boom Time for Cybercrime. *Consumer Reports*, 74 (June): 18–21.
- Delgadillo, Lucy M., Luke V. Erickson, and Kathleen W. Piercy. 2008. Disentangling the Differences Between Abusive and Predatory Lending: Professionals Perspectives. *Journal of Consumer Affairs*, 42 (Fall): 313–334.
- LaRose, Robert and Nora J. Rifon. 2007. Promoting I-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. *Journal of Consumer Affairs*, 41 (Spring): 127–149.
- Nehf, James P. 2007. Shopping for Privacy on the Internet. *Journal of Consumer Affairs*, 41 (Winter): 351–365.
- Norberg, Patricia A., Daniel R. Horne, and David A. Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, 41 (Summer): 100–126.
- Pitt, Leland F. and Richard T. Watson. 2007. A Reply [to Nehf]: An Ecosystem Perspective on Privacy. *Journal of Consumer Affairs*, 41 (Winter): 365–375.
- Rifon, Nora, Robert LaRose, and Sejung Marina Choi. 2005. Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures. *Journal of Consumer Affairs*, 39 (Winter): 339–362.
- Rotfeld, Herbert Jack. 2008. Financial Aliteracy. *Journal of Consumer Affairs*, 42 (Summer): 306–309.
- Rotfeld, Herbert Jack. 2009. Health Information Consumers Can't or Don't Want to Use. *Journal of Consumer Affairs*, 43 (Summer): 373–380.
- Turow, Joseph, Michael Hennessy, and Amy Bleakley. 2008. Consumers' Understanding of Privacy Rules in the Marketplace. *Journal of Consumer Affairs*, 42 (Fall): 411–424.
- Youn, Seounmi. 2008. Parental Influence and Teens' Attitudes Toward Online Privacy Protection. *Journal of Consumer Affairs*, 42 (Fall): 362–388.