Direct Marketing, Mobile Phones, and Consumer Privacy

James Nehf*

Professor King rightly observes that protecting consumer privacy in the United States is largely the responsibility of individuals. Although federal (and some state) laws restrict the collecting and sharing of personal information in some circumstances, restrictions are riddled with exceptions, and regulatory gaps are wide. Thus, we are left largely with market-based controls that have significant limitations.

Professor King's prescription for emerging privacy problems in the mobile phone industry is nuanced and multifaceted. Her principal arguments, however, for more transparency in the disclosure of privacy practices (e.g., clearer, multi-tiered privacy policies) and more open and volitional consumer consent to advertising and other privacy-invading activities (e.g., consent cannot be buried in the fine print of mobile phone contracts) fall short of what is necessary to protect consumers' interests.

On the surface, an enhanced notice-consent approach is appealing because it fits neatly within the consumer protection norm that has been dominant in the United States for several decades—better informed consumers can make rational decisions that correspond to their preferences, thereby promoting more efficient market outcomes than government dictates can provide. Her prescription makes perfect sense in this regard, but I question whether it will achieve the intended results. While better

* Professor of Law and Cleon H. Foust Fellow, Indiana University School of Law, Indianapolis. J.D., University of North Carolina; B.A., Knox College.

Suggested citation: James Nehf, *Direct Marketing, Mobile Phones, and Consumer Privacy*, 60 FED. COMM. L. J. F. 53 (2008), http://www.law.indiana.edu/fclj/pubs/v60/no2/NehfResponse.pdf.

notice and more volitional consent are worthy goals, my question is this: On what rational basis can consumers decide whether to opt in or opt out of a proposed privacy-reducing transaction? When faced with such a choice, consumers face several obstacles that make it difficult to value their privacy interests and make decisions that promote their best interests:

Valuing aggregation risks. To make an informed choice about whether and how to share personal information, people need to know what is at stake. Most people have no idea what information a phone company collects, how it will be aggregated with other data, and who will end up with the data at a later date. Disclosures in privacy policies, no matter how short and simple to read, cannot provide the necessary information. For example, a policy might say that the company shares only a limited amount of customer data and only with affiliated companies. But affiliated companies could be numerous and involved in entirely different lines of business, each with its own bits of information about the customer in its own database. Each likely will have its own set of information practices, unknowable to the phone customer. Or the company and its affiliates will obtain more information about individuals from a commercial data broker. Because even diligent mobile phone users lack the information necessary to evaluate the costs and benefits of information sharing bits of information that will be aggregated with other data, they rarely can evaluate the risk of a proposed information exchange.

Overcoming accountability problems. For phone users to protect their privacy interests and learn whether an information-sharing decision was good or bad, they must be able to identify the person who broke a law, breached a privacy policy, or allowed unauthorized access to its database because of lax security procedures. On the other side, businesses that collect data must fear that they will be exposed and held accountable if they do something wrong. There are two fundamental accountability problems that undermine both assumptions. First, individuals seldom know when a privacy breach has occurred. The vast majority of data collection—lawful and unlawful—occurs outside of public view. Although on occasion a breach of privacy norms results in media exposure, far more frequently, breaches remain hidden for months, years, or indefinitely.

Second, even if an injury or breach is detected, individuals may find it impossible to trace the problem to a particular cause or source. With personal information residing in countless databases, often there will be no way to locate the entity that caused a particular problem, sold the data, or permitted a hack or leak that ultimately caused someone to be harmed. Even with a noticeable harm such as identity theft, it may be impossible to learn how the thief obtained the personal information. Tracing the injury to the originating source often will be difficult or impossible.

Comparing incomparable values. When considering whether to trade personal information for some benefit, mobile phone users are faced with a fundamental incomparability among competing options. What is the value of knowing that the details of one's telephone usage will not be sold to third parties? Is it worth a ten dollar discount or an extra thirty Web browsing minutes per month? Comparing disparate categories of benefits and costs is difficult in any circumstance, but when making decisions about information privacy, the attributes we are asked to compare vary widely. Rather than struggle to make a difficult comparison, individuals usually turn to affect cues (feelings derived from a consumer's experiences with a particular alternative) and other heuristic devices (such as framing effects) as a decision making guide. For example, general feelings and attitudes resulting from a user's experience interacting with a phone company (e.g., its customer service reps seem friendly and honest) can affect decisions about sharing personal information, but those feelings can lead to inaccurate decisions because those feelings may not correlate with the company's actual privacy practices.

Pursuing conflicting goals. While consumers in controlled studies seem to value privacy and strive to protect it in their decisions about sharing information, their decisions about disclosing information in the real world usually do not match their stated privacy concerns.[1] Generally speaking, consumers make decisions under conditions of limited or bounded rationality, and decisions about sharing personal information are no different. People have a limited capacity for obtaining, understanding, and using information at every stage in a decision making process.

In making decisions, people pursue several, sometimes conflicting goals. One goal is accuracy of the decision: seeing that the outcome corresponds to the individual's set of preferences and priorities. But another important goal is the minimization of cognitive effort. People tend to expend only as much effort as is necessary to reach a satisfactory, rather than optimal, decision. As circumstances require more cognitive effort to process available information, decision makers choose decision methods that are easier to implement, though less accurate. The benefits of a multi-tiered privacy disclosure, for example, are therefore diminished because most consumers will not make the effort to learn the full story. If they bother to read the first-tier privacy policy, they will likely take their cue from the brief overview. Privacy notices for credit cards, for instance, often proclaim that the card issuer "cares about your privacy," but the

1. *See generally* James P. Nehf, *Shopping for Privacy Online: Consumer Decision Strategies and the Emerging Market for Information Privacy*, 2005 J. L., TECH. & POL'Y 1, 24, and references cited therein.

details of the collection and sharing practices can be found, if at all, only by the diligent consumer.

Another important goal in consumer decision making is minimizing the negative emotional response that people experience when they are forced to make difficult tradeoffs, and decisions about trading personal information for money or other benefits are difficult. People want to minimize the discomfort that arises from emotion-laden choices because they do not like being asked to trade sacred values for trivial returns. As a result, they tend to select simpler decision strategies. This can reduce the accuracy of the decision because an individual will avoid certain parts of the decision making calculus that require discomforting comparisons.

Lacking feedback. The more immediate and concrete the feedback about a particular decision making goal, the more emphasis one is likely to give it in making a decision. This is important in the market for privacy protection because the accuracy of any decision about revealing personal information usually will not be apparent until long after the transaction has ended. Indeed, feedback on the accuracy of the decision may never occur. With mobile phones, some consequences of a poor decision may be apparent in short order—for instance, the user may be deluged with more annoying than she had anticipated advertising. (Professor King's proposal that consumers should be able to change their opt-in decision is helpful in this regard). But only rarely will a consumer be able to trace other problems resulting from the decision—identity theft, consumer profiling, junk email or piles of snail mail—to the weak privacy practices of a particular mobile phone company or one of its affiliates or joint marketing firms. Without feedback about the decision, it is difficult to correct it or make a better decision when the next opportunity arises.

Professor King observes that notice and choice regimes are favorites of industry trade groups and their voluntary codes of practice. When voluntary codes are not enough, industry next favors notice and choice laws (particularly opt-out regimes) because they give the appearance of consumer sovereignty, and who can argue with that? While her prescription of enhanced disclosure of privacy practices and rules requiring more volitional consumer choice are an improvement on industry codes and the status quo, and her call for at least some opt-in rules should be heeded, the prescription might do little to protect consumers' privacy interests in the mobile phone industry. Mandatory limits on what information can be collected and how it can be shared may be necessary.

The standard criticism of mandatory controls is that they are likely to be less efficient than market-based measures. For a host of reasons, government regulators are not very good at setting the right balance of rights and responsibilities, and if they get it wrong, it takes time to correct.

The FTC and FCC have therefore hesitated to move with a heavy hand in this area. But there is little reason to believe that notice and choice will lead to more efficient results when it comes to privacy protection for mobile phone users. Indeed, the longer we wait to adopt mandatory controls, the more difficult it may be to overcome the influence of entrenched interests in the data collection industry. Professor King's thorough and well researched examination of this problem in its early stages is important and enlightening, but one cannot help but wish that she had explored a bolder set of remedies at this critical time when they would have a chance of gaining force.