Notice & Choice

Notice and Choice:

Implications for Digital Marketing to Youth

Paul M. Schwartz
University of California, Berkeley

Daniel Solove
George Washington University

Memo prepared for
The Second NPLAN/BMSG Meeting
on Digital Media and Marketing to Children

for the NPLAN Marketing to Children Learning Community

Berkeley, CA June 29 & 30, 2009

Sponsored by The Robert Wood Johnson Foundation

The Origins of Notice and Choice

The predominant way that privacy is protected in business records of consumer information is through an approach known as the "notice and choice." Notice and choice has its origins in the Fair Information Practices (FIPs), a set of principles for protecting information privacy that were first developed in an influential report by the Department of Housing, Education, and Welfare (HEW) in 1973. The principles include many individual protections, including (1) transparency of record systems, (2) collection and use of information that is accurate, relevant, and up to-date (data quality principle), (3) notice about what information was being collected about individuals, (4) a right to prevent information collected for one purpose from being used for other purposes, (5) a right to access one's personal information, (6) a right to correct erroneous information, and (7) data security protections.[1]

In contrast to Europe, where the FIPs were highly influential and led to omnibus privacy protections, the United States has adopted a more market-driven approach toward regulating consumer privacy. Businesses and marketers pushed the notice and choice approach, which selectively adopts only a few FIPs. Only the third FIP listed above survives in the notice and choice approach. The fourth FIP – often referred to as the purpose-specification principle – is recast as "choice." The idea behind notice and choice can be summarized in this fashion: As long as a company provides notice of its privacy practices, and people have some kind of choice about whether to provide the data or not, then privacy is sufficiently protected. This choice is not the robust right provided for in the fourth FIP above, but instead is often merely the ability to opt out of some information uses.

When the Internet started to blossom in the mid-1990s, companies created privacy policies that stated their practices with regard to how they collected, used, and disseminated personal data and offered people the ability to opt out of certain uses or disclosures of their information. This approach helped industry ward off legislation. Congress passed a few targeted laws to protect privacy in certain sectors, such as the Video Privacy Protection Act, which addresses the privacy of people's video entertainment choices and the Cable Communications Policy Act, which safeguards the privacy of cable records. But for most consumer information, such as data collected by merchants, supermarkets, bookstores, restaurants, and so on, Congress has yet to enact any sectoral laws.

Even existing laws that regulate privacy rely heavily on notice and choice. For example, the Children's Online Privacy Protection Act works primarily by requiring companies to have privacy policies to put parents on notice of how their children's data will be used and give them the choice to opt out, or indicate their refusal to "permit the operator's future use or maintenance in retrievable form, or future online collection, of personal information from that child."[2]

Instead of enactment of a full range of FIPs, regulators in the U.S. have predominately relied on the notice and choice approach. This path continued to be followed even after the EU Data Protection Directive raised vexing issues for the transfer of data between the United States and European Union (EU). The EU requires that countries to whom data is transferred provide an "adequate level" of privacy protection. A Safe Harbor Arrangement was established to enable data transfers between EU countries and the United States. The Safe Harbor Arrangement endorsed the notice and choice approach, a decision that received significant criticism in both the EU and United States.

Problems With Notice and Choice

Weak Enforcement

Notice and choice is by and large a self-regulatory approach. Companies are free to make whatever substantive promises they desire. Businesses can offer the consumer no privacy, bad levels of privacy, or strong privacy. The only consequences that companies face will occur should they violate the promises made in their privacy policies. Even some broken promises, however, go without penalty.

One consequence for breaching a privacy policy is a potential breach of contract action. However, the few courts that have considered the issue have concluded that (1) privacy policies are not really contracts, just statements by companies about their own practices; and (2) even if they were contracts, plaintiffs can rarely prove how they were harmed by the improper use or dissemination of their data.[3]

The other consequence for broken privacy promises is the potential for an Federal Trade Commission (FTC) action. Since 1998, the FTC has enforced the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce,"[4] to be violated when a company breaches its privacy policy. For the reasons discussed in our FTC memo, FTC enforcement has not been as effective as it should be.

Lack of Substantive Restrictions

As we have noted, a major problem with notice and choice is that it lacks any substantive restriction on what companies may do with personal information. All it requires is that companies follow their promises. But companies need not promise anything of note.

Lack of Real Notice

An additional major problem with notice and choice is that notice is illusory in practice. Privacy policies are long, cumbersome, and hard to read. Moreover, most people do not read privacy policies.

Moreover, privacy policies are often vague and unclear because they are drafted with the companies' self-interest in mind. There is little incentive for a company to provide specific notice as it will narrow that company's future potential use of information. Put differently, it is in the self-interest of companies to keep open their options, present and future, regarding use of personal information.

Another problem is that companies often reserve the right to make unilateral changes in their privacy policies. As a consequence, the privacy policy that you read today might not be the same you read tomorrow. And does anyone want to read a company's privacy policy on a daily basis? Given the vast number of companies collecting and using personal information today, it is unreasonable to expect people to read privacy policies for each one. It would be a full-time job to read and study them all, let alone continually check them and re-read them to learn about any changes.

Lack of Real Choice

On the choice side of notice and choice, some companies view choice as resting on allowing its customers the ability to opt out of certain data sharing and uses. Opt out sets the default as the company's right to use data however it desires unless a consumer indicates she does not want her data used or disclosed. Consumers can opt out by checking a box or taking other actions to indicate their "choice."

The problems with opt out are legion. Opt out is often cumbersome. Companies have no incentive to make opting out easy, and every incentive to make it difficult. Some companies will refresh people's preferences periodically, requiring them to opt out again and again if they want to remain opted out. Studies show that most people do not opt out – indeed, hardly anybody opts out – which is why companies prefer opt out so much.[5] It allows companies to shift burden and blame to consumers.

Moreover, the "choice" presented is more of a Hobson's choice than a real one. Many companies present consumers with a take-it-or-leave-it choice that provides hardly any ability for consumers to bargain about their privacy preferences.[6] If a consumer wants to buy a product, read a website, subscribe to a magazine, use a service, and so on, the consumer can be forced either to surrender privacy or to go elsewhere. But when nearly all companies offer the same take-it-or-leave-it approach, consumers desiring to protect their privacy have nowhere to turn.

What Can Be Done?

Therefore, in practice, notice and choice does not provide much notice or choice. It does create a façade of legitimacy for companies that allow them to take the actions that they desire with personal information.

The impact of the notice-and-choice regime will become even more negative for privacy in the context of behavioral marketing. These techniques provide a powerful new set of techniques with which companies can influence consumers. *There is no reason that behavioral marketing cannot be used as part of notice-and-choice to get consumers to refuse to opt out, or perhaps even to opt in.* An opt in system sets the defaults at restricted information use and disclosure, and only if an individual opts in will the company then be able to use the data.[7] We return to this issue regarding opt in below. Our point here is that if behavioral marketing is advertising on steroids, as it has been described, it can also make notice-and-choice even more effective in letting companies take the actions that they desire with personal information. Unless the current notice and choice approach is rethought, it might turn into a tool to permit companies to engage in behavioral marketing with hardly any restriction or oversight.

What regulatory regime should replace notice and choice? This is a very tricky question. Several factors make it difficult.

First, people lack expertise in privacy issues. It is difficult—if not impossible—for people to predict all the potential uses of their information, whether downstream or future.[8] Without knowing these uses, people cannot adequately assess the consequences of agreeing to certain present uses or disclosures of their data.

Second, the "aggregation effect" prevents people from making informed choices about the consequences of the collection and use of their data. The aggregation effect occurs when many pieces of seemingly innocuous data are combined to paint a more revealing portrait of an individual's personality.[9]

Third, many scholars and advocates argue for replacing opt out with opt in. Opt in is certainly an improvement over opt out under most circumstances. Yet, as we have warned above, even under an opt in system, companies can sometimes readily find ways to get people to opt in. For example, supermarket and drug store discount cards get people to relinquish vast amounts of personal data in exchange for saving money. Empirical studies show that people are willing to trade their personal data for small rewards.[10] Behavioral economists Alessandro Acquisti and Jens Grossklags explain that information asymmetries (where people lack knowledge of how their data will be used) and bounded rationality (where people have trouble dealing with complex situations) explain why people are so willing to readily relinquish their personal data.[11] As we have noted, behavioral marketing is likely to greatly heighten this effect.

Fourth, on the other side of the ledger is the complex issue of paternalism. Some people want to be the targets of marketing. These individuals want their data shared; they enjoy receiving ads targeted to their interests. For example, many people enjoy Amazon.com's recommendations system, which uses an individual's personal data to generate lists of books, movies, music, and other items they might find interesting. Many people find this service useful. A law that restricted certain forms of marketing might prevent people who consent and desire marketing from receiving the information that they desire.

So what should be done? A system based on notice and choice has shown itself to be ineffective, and certain problems make solutions relying on people's purported "consent" to be dubious. On the other hand, paternalistic regulation may override some people's consent. One pragmatic solution might involve some combination of consent and paternalistic regulation.

As a series of "thought experiments," we wish to propose a broad range of ideas for debate and discussion:

1. ***Fortified Opt In.*** An opt in system with certain protections might address some of the problems with opt in. Companies should not be allowed to make the provision of access, information, services, or transactions contingent upon a person's opting in.
2. ***Standardized Notice.*** A privacy notice label, akin to that required for food nutritional information, should be mandated so that people can more readily understand and compare privacy policies. Some companies are already experimenting in this spirit, and creating "layered" privacy notices.
3. ***Universal Notice.*** Companies should be required to register their privacy practices with the FTC, which will put all of them on a centralized website, where consumers can readily see and compare them.
4. ***Reviving the Purpose Specification Principle.*** A principle of the FIPs conveniently dropped out by industry is the principle of "purpose specification" – that information collected for one purpose should not be used for another purpose without the individual's consent. This principle is a cornerstone of European privacy law. It should be revived and implemented in U.S. privacy law.
5. ***Importing Concepts Akin to Restrictive Covenants and Easements into Personal Data.*** In property law, certain rights and restrictions "run with the land" – they are affixed to a piece of property and go along with it whenever ownership is transferred. For example, an easement which allows people to cross a person's property can be permanently affixed to that land. Something similar should apply to personal information –

people's rights should be automatically affixed to it, and they should travel with it whenever the information is transferred.[12]

6. ***Universal Opt Out.*** Currently, it is difficult to opt out of data sharing since so many companies are gathering and sharing personal data. The FTC might maintain a system where a person can universally opt out of all data sharing by every company that uses their data.
7. ***Accountability and Enforcement.*** One of the reasons companies can so readily use personal information is that the law does not require them to internalize all the costs it creates. If companies were strictly liable for data security breaches and other harms created when people's data was misused, they would fully internalize the costs of using personal information and might use it more sparingly.
8. ***Liquidated Damages for Privacy Violations.*** Many courts fail to recognize privacy harms when data is leaked, when privacy policies are violated, or other instances when companies improperly use or reveal people's information. As a result, there isn't an adequate legal deterrent, and this drastically lowers the price for using personal information. Strong liquidated damages provisions for privacy violations will force companies to internalize the full cost of their activities.
9. ***Restrictions of Certain Types of Behavioral Marketing.*** Certain uses of data and types of data and kinds of behavioral marketing should be restricted outright. Such practices might include marketing to children and teenagers, a population especially vulnerable to the influences of behavioral marketing.
10. ***Transparency.*** Companies engaging in certain kinds of behavioral marketing should be required to submit a filing about their practices to the FTC, which will review their marketing plans and ensure that privacy is adequately protected. Such marketing should only take place with the approval of the FTC. Such a system can work akin to securities regulation or the regulation of pharmaceuticals.

###

References

[1] U.S. Dep't of Health, Education, & Welfare, *Records, Computers, and the Rights of Citizens* 41-42 (1973). For a recent discussion of FIPs, see Paul M. Schwartz, Preemption and Privacy, 118 Yale L.J. 908, 909-910 (2009).

[2] Children's Online Privacy Protection Act, 15 U.S.C. § 6502(b)(1)(B).

[3] See Dyer v. Northwest Airlines Corp, 334 F. Supp.2d 1196 (D.N.D. 2004); In re Northwest Airlines Privacy Litigation, 2004 WL 1278459 (D. Minn. 2004); In re JetBlue Airways Corp. Privacy Litigation, 379 F.Supp.2d 299 (E.D.N.Y. 2005).

[4] 15 U.S.C. § 45.

[5] Russell Korobkin, *Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms,* 51 Vand. L. Rev. 1583 (1998) (observing that most people accept default terms).

[6] Paul M. Schwartz, *Privacy and Democracy in Cyberspace,* 52 Vand. L. Rev. 1609, 1662 (1999).

[7] See generally Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information,* 74 Wash. L. Rev. 1033 (1999).

[8] Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* 84-86 (2004).

[9] *Id.* at 87-88.

[10] Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Decision Making,* IEEE, Security and Privacy 24 (2005).

[11] *Id.*

[12] Paul M. Schwartz, *Property, Privacy, and Personal Data,* 117 Harvard Law Review 2055 (2004).