

PRIVACY: FINDING A BALANCED APPROACH TO CONSUMER OPTIONS

Robert Gellman, Privacy and Information Policy Consultant
rgellman@netacc.net

This paper discusses two issues central to current debates about privacy: 1) consumer choice regarding secondary use of personal information collected by record keepers; and 2) application of opt-in or opt-out rules for determining how personal information can be used and disclosed.

In any discussion of public policy, framing the issues is essential because beginning the debate from the wrong starting point may lead to a pre-ordained conclusion and preclude consideration of important alternatives. The framing of the choice and opt-in/out issues offers a good example of how the debate has been skewed and unbalanced.

Choice is not a core privacy principle. It is a concept typically advanced by business institutions that abridges longstanding American principles of fair information practices[1] – principles that form the basis of domestic laws and have been incorporated into international codes and the laws of foreign countries.[2] The concept of choice degrades principles offering fairer protections for consumers – *purpose specification*, *use limitation*, and *consent*.

The debate over opt-in and opt-out is similarly flawed. Privacy alternatives cannot be easily stuffed into these two crude, poorly-defined, and misleading categories. This paper shows how framing the issues in terms of choice and opt-in/opt-out distorts the analysis and leads to diminished protections for consumers.

Choice Is the Wrong Starting Place. Purpose Specification is the Right Place.

Choice is a policy that favors record keepers over record subjects. The main feature of choice allows a record keeper to use or disclose personal information as long as the record subject has some ability to express a preference. At its worst, choice can be implemented so that personal information may be used in any manner that a record keeper wishes as long as the record subject has been offered some opportunity to object to its use, no matter how limited or difficult it may be to exercise that option. Choice can also allow a record keeper at any time to redefine use and disclosure practices for personal data. When discussions of privacy include choice as a core principle, the data subject is placed at an immediate disadvantage.

Initially, it would seem reasonable that consumers should have a choice about how their data may be used. Choice has a place in the privacy balance. However, choice is not a fundamental privacy principle in most countries around the world. It is not the right place to start.

A fair analysis of privacy policy must begin with more comprehensive principles. Missing from the concept of choice is the important idea that a record keeper must state a *purpose specification* – a clearly defined statement of the purpose for collecting, maintaining, using, and disclosing

[1] Fair information practices were developed in the United States in 1973 by a federal advisory committee. See Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, (1973) (Department of Health, Education & Welfare), at <<http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm>>.

[2] A restatement and refinement of fair information practices by the Organization for Economic Cooperation and Development in 1980 strongly influenced legislatures in Europe and elsewhere around the world. See *Council Recommendations Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 20 I.L.M. 422 (1981), O.E.C.D. Doc. C (80) 58 (Final) (Oct. 1, 1980), at <<http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>>.

personal information. Most privacy policies and laws around the world require purpose specification rather than choice.

A statement of purpose helps to strike a reasonable balance between the interests of record keepers and those of record subjects. It tells the record subject the consequences of disclosing data. For example, a product warranty card often asks for personal information about the purchaser, but it seldom says how the information will be used or whether the data is necessary for a warranty to be valid. The rarely told truth is that the information collected is often shared with other companies and used for marketing and profiling. The warranty is usually just as valid even if a consumer never returns the card.

A purpose statement provides the data subject with information about the purpose for data collection, so that he or she can assess the benefits and risks of disclosure and make an informed decision. It also prevents a record keeper from using or disclosing information in ways that are not in accordance with the stated purpose. A warranty card that does not have a statement of purpose is unfair to consumers.

The purpose specification principle has a self-balancing feature. A record keeper who states a broad purpose (“we will make any use or disclosure that is profitable”) or an unpopular purpose (“we will sell your telephone number to telemarketers who call you at home”) runs the risk that people will take their business and their information elsewhere. On the other hand, a narrow purpose statement affirming that personal information will be used fairly may encourage people to enter into a business relationship.

How detailed a purpose statement should be is open to interpretation. An activity that is compatible with a stated purpose should be permissible if the relationship between the purpose and the new activity does not exceed the reasonable expectation of consumers. For example, most bank customers would consider the use of depositor records to support an automatic teller machine network to be reasonable. On the other hand, consider a bank that shares depositor account numbers and balances with a telemarketer in exchange for a percentage of revenue generated by sales calls. The sale of depositor information is not something that most

consumers expect when they open a bank account. A bank that wants to engage in that type of sharing should tell consumers so that they can make an informed decision about whether to do business with the bank.

Use limitation is another core principle that, together with purpose specification, maintains a balance between the interests of the record keeper and those of the record subject. The use limitation principle provides that personal information should not be used or disclosed except for the purpose specified at the time of collection. The use limitation principle enforces the promise made by the purpose specification. Exceptions are permitted with the consent of the data subject or when authorized by law.

The Role for Consumer Preferences

Once a record keeper specifies a purpose, choice becomes relevant in two ways. First, when a record keeper states the purpose for personal information collection, any new use or disclosure generally requires the affirmative consent of the record subject. When a new activity is inconsistent with the terms under which the record keeper established a relationship with the record subject, the record keeper must seek affirmative approval from the record subject. Another term for affirmative approval is *consent*.

Second, choice can be an element of a record keeper’s purpose specification. For example, a magazine publisher can tell consumers that it will use the consumer’s subscription information to fulfill the subscription and to send the consumer offers for other magazines. The publisher can present the consumer with a single option, namely subscribe to and receive other offers. The publisher who fears losing business from those who don’t want to receive mail, phone calls, or spam might find it prudent to give consumers more options. The publisher may tell subscribers that they can buy the magazine and not receive other offers. Presenting that option is one way that a record keeper can accommodate the preferences of consumers. Consumers receive a clear choice within the framework of defined purposes, and personal information is not subject to additional uses at the whim of the record keeper.

The Complexities of Opt-in and Opt-Out

Consumer choice is often presented as either an *opt-in* or an *opt-out*. “Opt-in” means that information will not be used unless the record subject affirmatively gives consent. “Opt-out” means that information will be used unless the record subject states an objection. Both opt-in and opt-out provide guidance to a record keeper in the absence of a clear preference from a record subject. Typically, consumers accept the default policy. This means that opt-in will mostly limit data use because few consumers will opt-in. If the policy is opt-out, few consumers will opt-out, and their data will be available for secondary uses.

Characterizing consumer choice as opt-in or opt-out is overly simplistic and significantly misleading. The issue is more complex, and more factors are relevant to an evaluation of the fairness of any exercise of consumer choice. Without considering these other factors, identifying an option as opt-in or opt-out will not provide enough information to assess whether the process achieves the appropriate balance between the interests of consumers and those of companies collecting information.

The terminology is also confusing when record keepers mix up the terms. Some say that a consumer who hasn’t opted out has actually opted in. The result is that neither term has a clear meaning.

A preliminary issue is whether we need a default rule at all. If consumers always express a preference, then neither opt-in nor opt-out is necessary. However, in many circumstances it can be impossible to make consumers choose. They may ignore a letter or refuse to check off a box on a form. Only when consumers do not speak is a default policy needed.

Consider, for example, a website that requires that users register to obtain access. The registration page asks for information before allowing the user to enter the site. That page can demand that a user choose between two (or more) options about reuse of personal information. Until the user makes a choice, he or she cannot advance to the next screen and complete the registration. The result is that each registered user states a preference, and no default rule is necessary.

Factors for Evaluating the Fairness of an Opt-in or Opt-out

Once we determine that a default rule is appropriate, many factors are relevant to assessing the options presented to consumers.

- **Pre-Checked Box.** What is the difference between opt-in and opt-out on a website? Consider a registration page on a website that asks users to decide whether to allow secondary use of their personal information or no secondary use. Suppose that the box indicating one of the alternatives is pre-checked. The user who clicks to the next page gets the default selection, although the ability to change the selection remains.

If the box that allows secondary use is pre-checked, is that opt-out? If the box prohibiting secondary use is pre-checked, is that opt-in? Whether a box is pre-checked and which box is pre-checked is a very small difference to support the notion that opt-in and opt-out offer starkly different policies. It is hard to decide what is the fairest characterization without considering some of the other factors discussed below.

- **Usage.** How will the information be used and shared? Compare an opt-out that limits reuse of an email address to a once-a-year marketing message with an opt-in that allows unlimited reuse and resale of all personal data, including medical and financial information. Of these two alternatives, the limited opt-out policy may be a fairer and more balanced deal for consumers than the unrestricted opt-in policy. Assuming that opt-in is always more protective of consumer privacy than opt-out may not be true.
- **Notice.** What information does a record subject receive when making a choice? If a notice is incomplete, misleading, hard to find, or difficult for the average consumer to understand, the options may be unfairly presented regardless of other considerations. Warranty cards are examples of opt-in devices that rarely inform consumers of the full consequences of filling out and returning the cards.

- **Timing.** Must consumer receive notice before the record keeper can make any secondary use of the data? The answer may depend on the nature of the relationship between the record keeper and the record subject. A physician may always begin a relationship with a patient with a face-to-face meeting so prior notice may be practical. That may not always be the case for other types of businesses.
- **Sensitivity.** Does the type of personal information make a difference when deciding about a fair choice? Should a record keeper that collects medical or financial information use an opt-out policy? Consider a hospital or HMO that establishes an opt-out policy and buries the opt-out notice in the middle of a long set of forms. Would it be fair to allow disclosure of a patient's entire medical history to marketers without restriction if the patient didn't see the notice and failed to object? Many countries require clear and affirmative consent before permitting any secondary use of sensitive personal information (*e.g.*, health, sexual preference, and religion).
- **Granularity.** Are options linked to other activities? Requiring a patient to authorize both medical treatment and secondary use with a single signature would be an example of an unfair opt-in that does not offer sufficient alternatives.
- **Form.** What form of response by the data subject is required? Composing and snail-mailing a letter is a major barrier for most people. Existing financial privacy rules recognize that asking consumers to opt out by composing and mailing letters is an unreasonable burden. A check-off box, postpaid envelope, preprinted form, or toll-free number may present consumers with a fairer opportunity to exercise a decision. The amount of information that a consumer must provide to opt out may also be a factor. For example, asking consumers to disclose a Social Security or credit card number as a required element of an opt-out is sure to discourage many people.
- **Verification.** When a user opts in on a website or through email, should there be

a subsequent verification from the user? Many email users receive spam from a sender who contends that the user opted in to the solicitation. Yet this is not always true. When and how should an opt-in be verified?

- **Cost.** Must a record subject pay to opt out? Some who offer opt-out services require consumers to pay in order to have their names removed from lists. Consumers should always be able to exercise choice free of charge. Consumers have that right by law in Europe and in other countries.
- **Duration.** How long is an opt-out effective? If an opt-out expires after a year and then must be renewed at the initiative of the consumer, is that a fair opt-out? An expiring opt-out may be a ploy to lead consumers to believe that they have stopped secondary use when the effect is to trap unwary or inattentive consumers.
- **Change.** How can a consumer change a choice already made? If a consumer need only visit a website and check a box, the method may be reasonable, at least for consumer with Internet access. In other circumstances, a business can make it burdensome for consumers to change their minds.

Consider, however, a transaction that typically takes place in the physical presence of the consumer and a business. An example is a contract between a consumer and a real estate agent for the sale of a house. Suppose that the contract asks a consumer to opt in to reuse of information for marketing. Reasonably presented, the choice may be fair. Suppose that a consumer now wants to opt out. If the consumer must make the change in the same way as the original decision, the consumer might have to physically meet the agent to request the change. It may be impossible or impractical for consumers to change their minds. A policy that all consumer choices be made in the same way – even if that way is through affirmative choice – can still be unfair to consumers.

Conclusion

Finding a balanced approach to privacy concerns is essential today. Individuals must share personal information to function in our complex, interconnected society. Many institutions, organizations, and businesses routinely collect personal data as an essential part of their operations. Societal objectives, such as law enforcement, national security, public health, and economic growth, sometimes require that information be available for secondary uses regardless of the wishes of the data subject. In many other circumstances, however, individuals should be able to exercise some control over their personal information.

In approaching privacy, it is important to understand the ever-increasing demands of record keepers for personal information to be used for profiling, sharing, marketing, and for other purposes that are secondary to the reason the information is collected in the first place. The interests of consumers in controlling personal information must also be recognized. Balancing all of the rights and interests that are part of privacy is rarely simple. What is essential is that debates over privacy policy not start out favoring one side or the other.

Consumer choice has a role in how businesses and others process personal information, but it is not the place to start when developing privacy policy. Record keepers should first define the purpose of their activities and then live within the constraints that they establish. Record subjects can and should exercise choice, but only within that framework. The goal is fairness and balance. Choice is an element in meeting that goal, but it is not an independent objective. A privacy policy with choice as a central principle will unduly favor record keepers over record subjects.

“Opt-in” and “opt-out” are terms widely used in privacy discussions, but the shorthand terminology hides the complexity. It is not practical to divide the privacy world into two simple alternatives called opt-in and opt-out. When we must rely on a default rule for determining consumer choice, other factors must be evaluated, including scope, notice, timing, sensitivity, granularity, form, verification, cost, duration and change. The goal is to find a fair approach that recognizes privacy rights and interests and that balances them appropriately against other relevant rights and interests.