

# Conceptualizing Information Privacy and Information Regulation

MICHAEL YOUNG\*

## I. INTRODUCTION

Contemporary information technology does not so much *create* as *reveal* a concern to avoid violations of personal privacy. If we did not already recognize privacy as a value, we would not recognize that contemporary technology potentially implicates that value. This suggests that any question of the form “how can we preserve our privacy in the face of information technology x?” (including the question “how should we regulate online behavioral marketing?”) can be conceptualized as an instance of a more general problem or concern to preserve what may be called “informational privacy.” This paper first deconstructs some of the nature of this more general concern; hopefully, this adds something to an understanding of the over-arching issues. Second, in keeping with the initial analysis, this paper sketches out a regulatory program that aims to preserve informational privacy *without* focusing on particular technology itself.

## II. INFORMATION PRIVACY: NON-EXPOSURE AND NON-MISUSE INTERESTS

The concept of “information privacy” identifies two potentially distinct interests. First, we have an interest in not being personally exposed in some way, as by the revelation of a personal secret. Call this our *non-exposure* interest. *Being exposed* counts as a worrying violation of *ourselves*, and we further think that *being exposed* can occur given merely the disclosure of certain information about us to other people.

Our second interest in information privacy is the concern to prevent harm by the misuse of information connected to us. This gives rise to what may be called a *non-misuse* interest; we do not want information disclosed to someone who will use it as an instrument of harm. We generally want to keep our social security, bank account, and credit card numbers private

\* J.D. anticipated, 2010. The author may be contacted at [yon-ansbach-youn.1@osu.edu](mailto:yon-ansbach-youn.1@osu.edu). This paper was written for Peter Swire’s fall 2008 *Cyberspace* seminar at the Moritz College of Law.

because the disclosure of this information facilitates fraud (such as identity theft). Where the non-misuse interest is violated, it is plausible to think that it is not disclosure *itself* that is the harm, but the fact that the disclosure makes some mischief a living possibility. Thus, if we could be absolutely certain that the information would not be misused, we would not likely care at all that our various private numbers were revealed for all to see.

The problem of protecting our non-exposure interest is trickier than the problem of protecting our non-misuse interest because it is very difficult to say in advance precisely what counts as *being exposed* for any particular person. In contrast, we seem to have some clear idea of what kinds of information disclosure would universally count as violating the *non-misuse* interest of nearly any person – certainly, this includes the disclosure of social security, bank account, or credit card information to untrustworthy people. We lack the same grip on the precise kinds of information disclosure that would similarly implicate the *non-exposure* interest of nearly any person. I may not care if the world knows my sexual orientation; you may care very much. I may be willing to expose my embarrassing medical condition in a limited way if it means an easier time finding a cure or helpful medicine; you may prefer suffering in silence. I may worry that my family knows something about me but be unconcerned that a perfect stranger knows the very same thing; you may be more free with your family and more wary of strangers. In short, in the case of the non-exposure interest, it is simply not clear which generalizations will be valid.<sup>1</sup>

The regulatory problem posed by the very particularity and idiosyncraticity of the non-exposure interest should be obvious. An inability to confidently say in advance what in particular

---

<sup>1</sup> See, e.g., HARRIS INTERACTIVE, MAJORITY UNCOMFORTABLE WITH WEBSITES CUSTOMIZING CONTENT BASED VISITORS PERSONAL PROFILES: LEVEL OF COMFORT INCREASES WHEN PRIVACY SAFEGUARDS INTRODUCED (April 10, 2008), *available at* [http://www.harrisinteractive.com/harris\\_poll/index.asp?PID=894](http://www.harrisinteractive.com/harris_poll/index.asp?PID=894). This poll shows that popular attitudes toward the practices of online behavioral marketers can shift given various privacy safeguards, but, even so, the numbers indicate relatively narrow majorities on the posed questions. This suggests sizeable and meaningful variation in underlying individual preferences.

answers to the description of *being exposed* limits the kinds of general rules we can formulate with that end in mind, at least if we want to avoid excessively over- or under- broad regulation.

### III. SKETCHING A REGULATORY SCHEME

We can turn now to an outline sketch of a regulatory scheme. The non-misuse interest can be protected by requiring, as regards sensitive numbers or passwords susceptible to misuse, that there should be:

- a) No collection of such information unless the information-target<sup>2</sup> has expressly provided (or consented to the provision of) such information to the entity.
- b) No further disclosure of such information except to trustworthy entities. (Obviously, legally defining “trustworthy” is problematic, but should include established business-to-business service providers, like payment processors.)
- c) Strict liability for inadvertent disclosure. (And perhaps a private federal right of action to aid enforcement.)
- d) Strict liability for any direct fraudulent use of the provided information.

Admittedly, as presently constructed, these standards are vague. Nevertheless, the overarching point should be clear; the point is to limit the collection of data susceptible to fraudulent misuse in the first instance, and to make the data collector strictly liable for information systems which do not maintain the sensitive data in an adequately secure way.

If the non-exposure interest is to be protected without creating over- or under- broad categories, then the particular idiosyncratic preferences of the information-target must be identified and respected. One way to accomplish this is by giving the information-target a meaningful opportunity to elect *not* to have the information he provides (in one way or another) disclosed to another person; presumably, the information-target will know whether he has a preference to disclose or not. If the notice was conspicuous and readily understandable enough, it should not matter, from the viewpoint of the non-exposure interest, whether the election was opt-

---

<sup>2</sup> ‘Information-target’ means here ‘a person from whom information is / was gleaned.’

in or opt-out. Opt-out consent is strong enough to protect the non-exposure interest, provided the information target is aware of his own preferences and aware of the notice and his choice.<sup>3</sup>

Incidentally, it should not matter just at *what* point the chance to opt-out occurs, so long as it occurs before the information in question is potentially disclosed to another person. And, if there is some technological system whereby the information associated with the information-target *could not* be disclosed to any person (other than the information-target himself), then the exposure-interest is already protected, without any need for notice and consent.

Of course, defining “potential disclosure” is non-trivial, but, as a first gesture, it should be understood broadly. It should include the provision of information identified with a particular person to a third-party marketer. (For example, this would be the case where an offline marketing services company provides to a marketer a names-and-address list of people likely to be interested in this or that product.) And in targeting advertisements at a particular person, information is “potentially disclosed” to anyone else who might see the targeted ads.

In keeping with these ideas, regulation aimed at protecting the non-exposure interest could be structured around the following points:

- a) Entities which potentially disclose information associated with and ultimately collected from a particular person must, prior to any such potential disclosure, be required to assert that the person connected to the data has a) been reasonably notified of such potential disclosure in the manner prescribed by this section, b) had a concurrent, immediate, and clear chance to opt-out, and c) failed to opt-out.
- b) Notice and a chance to opt-out must appear together, and there must be no monetary cost associated with opting out.
- c) The transaction exception: when actual or potential disclosure is necessary to (or contemplated by) the accomplishment of a transaction initiated or explicitly agreed-to by the information-target, the above provisions shall not apply.

---

<sup>3</sup> There are reasons why opt-out might be preferred – where a person is agnostic about their preferences, opt-out sets the default presumption in favor of extracting value from information by those (such as marketers) in a position to do so. *See* Michael Young, Perception, Reality, and the Regulation of Online Behavioral Marketing, 4-5, 12-14 (Nov. 26, 2008) (unpublished seminar paper) (on file with the author).

- d) The interaction exception: no entity shall be liable under this section for the disclosure of information incidentally to or in the course of an interaction initiated by or consented to by the information target. (The idea here is for an exception which allows intuitively harmless practices such as contextual advertising.)

Under this scheme, online behavioral marketers ordinarily would have to provide notice and an opportunity to opt-out. But this is accomplished through rules applying equally to other technologies and media. Under the broad definition of “potential disclosure,” targeted ads served by a behavioral marketer could disclose information about me, unless the marketer can (somehow) guarantee that I will be the only person to see those ads, and that nobody else will otherwise have access to information about me. (If that *were* the case, my non-exposure interest would not be implicated.) Consequently, the notice and consent provisions apply.

#### IV. CONCLUSION

The above sketch of a proposal aims to protect our informational privacy interests by regulating at the level of potential and actual information *disclosure*. Since it is ultimately unwanted disclosure of information to other persons which violates our interests in informational privacy, this would seem to be the most naturally appropriate level of abstraction at which to regulate. The suggested scheme also attempts to account for the idiosyncraticity of the non-exposure interest; the point of *notice* and *choice* here is not that there is some mystical value attached to these things, but that these are the means by which the idiosyncratic non-exposure interest can be protected. Where we have strong intuitions that some practice does *not* implicate privacy concerns (such as contextual advertising), the point is to find a general description, above the level of particular technology, encompassing these intuitions. If this particular offered regulatory outline is rejected (and it is admittedly under-specified), these broad aims should nevertheless be kept in mind when framing an alternative.