February 4, 2013

Privacy, Transparency & Google's Blurred Glass

Jonathan I Ezor, Touro Law Center

Available at: https://works.bepress.com/jonathan_ezor/10/
No matter the context or jurisdiction, one concept underlies every view of the best practices in data privacy: transparency. The mandate to disclose what personal information is collected, how it is used, and with whom and for what purpose it is shared, is essential to enable informed consent to the collection, along with the other user rights that constitute privacy best practices. That disclosure may be to governmental agencies as well as the users themselves, but the ultimate goal is that the users will know what information from and about them is being collected by the organizations with which they interact.

The FTC’s Fair Information Practice Principles provide a concise definition and explanation of the need for transparency, in discussing the primary principle, “Notice/Awareness”:

*The most fundamental principle is notice. Consumers should be given notice of an entity’s information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information. Moreover, three of the other principles discussed below -- choice/consent, access/participation, and enforcement/redress -- are only meaningful when a consumer has notice of an entity’s policies, and his or her rights with respect thereto.*

*While the scope and content of notice will depend on the entity’s substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:*  
  identification of the entity collecting the data;  
  identification of the uses to which the data will be put;  
  identification of any potential recipients of the data;  
  the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);  
  whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and  
  the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.  
*Some information practice codes state that the notice should also identify any available consumer rights, including: any choice respecting the use of the*
data; whether the consumer has been given a right of access to the data; the
ability of the consumer to contest inaccuracies; the availability of redress for
violations of the practice code; and how such rights can be exercised.

In the Internet context, notice can be accomplished easily by the posting of
an information practice disclosure describing an entity's information practices on
a company's site on the Web. To be effective, such a disclosure should be clear
and conspicuous, posted in a prominent location, and readily accessible from
both the site's home page and any Web page where information is collected from
the consumer. It should also be unavoidable and understandable so that it gives
consumers meaningful and effective notice of what will happen to the personal
information they are asked to divulge.¹

Another example, from the Consumer Privacy Bill of Rights issued by the Obama
Administration, states:

**TRANSPARENCY:** Consumers have a right to easily understandable
and accessible information about privacy and security practices. At times and
in places that are most useful to enabling consumers to gain a meaningful
understanding of privacy risks and the ability to exercise Individual Control,
companies should provide clear descriptions of what personal data they collect,
why they need the data, how they will use it, when they will delete the data or de-
identify it from consumers, and whether and for what purposes they may share
personal data with third parties.

Plain language statements about personal data collection, use, disclosure,
and retention help consumers understand the terms surrounding commercial
interactions. Companies should make these statements visible to consumers when
they are most relevant to understanding privacy risks and easily accessible when
called for.

Personal data uses that are not consistent with the context of a company-
to-consumer transaction or relationship deserve more prominent disclosure than
uses that are integral to or commonly accepted in that context. Privacy notices
that distinguish personal data uses along these lines will better inform consumers
of personal data uses that they have not anticipated, compared to many current
privacy notices that generally give equal emphasis to all potential personal data
uses.² Such notices will give privacy-conscious consumers easy access to
information that is relevant to them. They may also promote greater consistency
in disclosures by companies in a given market and attract the attention of
consumers who ordinarily would ignore privacy notices, potentially making
privacy practices a more salient point of competition among different products
and services.

In addition, companies should provide notice in a form that is easy to read
on the devices that consumers actually use to access their services. In particular,

¹ FAIR INFORMATION PRACTICE PRINCIPLES, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited
Feb 4, 2013).
mobile devices have small screens that make reading full privacy notices effectively impossible. Companies should therefore strive to present mobile consumers with the most relevant information in a manner that takes into account mobile device characteristics, such as small display sizes and privacy risks that are specific to mobile devices.

Finally, companies that do not interact directly with consumers—such as the data brokers discussed above—need to make available explicit explanations of how they acquire, use, and disclose personal data. These companies may need to compensate for the lack of a direct relationship when making these explanations available, for example by posting them on their websites or other publicly accessible locations. Moreover, companies that have first-party relationships with consumers should disclose specifically the purpose(s) for which they provide personal data to third parties, help consumers to understand the nature of those third parties’ activities, and whether those third parties are bound to limit their use of the data to achieving those purposes. This gives consumers a more tractable task of assessing whether to engage with a single entity, rather than trying to understand what personal data third parties—potentially dozens, or even hundreds—receive and how they use it. Similarly, first parties could create greater transparency by disclosing what kinds of personal data they obtain from third parties, who the third parties are, and how they use this data. This level of transparency may also facilitate the development within the private sector of innovative privacy-enhancing technologies and guidance that consumers can use to protect their privacy.

The European Union’s Data Protection Directive\(^2\) mandates disclosure in Section IV, Art. 10:

> Member States shall provide that the controller [the party collecting the personal information] or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:
> (a) the identity of the controller and of his representative, if any;
> (b) the purposes of the processing for which the data are intended;
> (c) any further information such as
> - the recipients or categories of recipients of the data,
> - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
> - the existence of the right of access to and the right to rectify the data concerning him
> in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

---
Transparency of data collection is also a key part of the best practices long recommended by advocacy groups including the Electronic Privacy Information Center, the Electronic Frontier Foundation, and the Future of Privacy Forum.

Similarly, transparency has become a key word for companies’ discussions of their own data practices. Notably, Google, whose business goes far beyond its original focus on online search, publishes a semi-annual Transparency Report disclosing the number and disposition of government requests of information from Google, along with other statistics such as content removal requests. Twitter, the social network, has recently begun publishing its own Transparency Report, following Google’s lead.

Google, however, is far from transparent, regardless of its report titling, and the issue is a significant one for user privacy. The challenge comes from the sheer diversity of Google’s operations, and the resulting large number of channels through which Google may be collecting and collating user information. Google makes reference to this in its own privacy policy:

There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we’re using information and the ways in which you can protect your privacy.

Google further states, “Our Privacy Policy applies to all of the services offered by Google Inc. and its affiliates, including services offered on other sites (such as our advertising services),

---

but excludes services that have separate privacy policies that do not incorporate this Privacy Policy.”

For all its stated dedication to transparency, however, Google makes it almost impossible to discover the entire range of products, services and brands it owns and control, and through which it is collecting user information. The company’s Products page lists categories including Web, Mobile, Media, Geo (geographic), Home & Office, Social, Specialized Search, and Innovation, and includes products such as Orkut, Blogger, and Picasa whose names might not immediately identify them as Google services. The list is far from detailed; the link to Mobile leads to another page which briefly describes the Android operating system owned and licensed by Google and running on devices from many manufacturers, the Google-branded Nexus devices, and further links to Google apps running on both Android and Apple’s iOS operating system.

More seriously, though, the lists on these pages are woefully incomplete. Google owns numerous businesses operating under other brand names, and is constantly acquiring others. Among the popular consumer brands that are owned and operated by Google, and therefore could be feeding information into the central Google databases, are the hardware manufacturer Motorola Mobility, the restaurant guide Zagat, and Frommer’s, the well-known travel publisher; the latter two link to Google’s privacy policy as their own. Ironically, one way to discover some of Google’s other products is through a Google search, while another less-than-authoritative resource is Wikipedia. Google also provides GPS-supplementing location data derived from mapped WiFi hotspots and access points to its own operating system and others such as Apple, derived from information transmitted by Android devices back to Google whether

---

10 Id.
16 https://www.google.com/search?q="acquired+by+google"+OR+"owned+by+google".
or not users are aware of the collection (and even where it is the location of the users’ own WiFi routers being sent).  

Google’s famous corporate motto, enshrined in its Code of Conduct, is “Don’t be evil,” and neither its collection or use of personal information is necessarily malicious. It is, though, clearly the driver of its overall business model, and therefore Google is always incentivized to find new channels through which to collect and combine information about users. Among the company’s “Ten Things We Know to Be True” are two statements which resonate somewhat ironically given the lack of true transparency when it comes to Google’s data practices: “Focus on the user and all else will follow” at number 1, and “There’s always more information out there” at number 7. (“You can make money without doing evil” is number 6.) Google also acknowledges that its efforts at transparency through its user account Dashboard, are incomplete, where it states: “Is this everything? In a nutshell, not yet.”

Whatever Google’s good intentions, and its stated desire to promote transparency as an ideal, the company remains seriously deficient in its actual disclosure to its users about its personal information collection and use practices, even as its servers gather more data through more channels and sources about more users around the world. When the Federal Trade Commission recently announced the settlement of its investigation into Google, it largely focused on Google’s alleged power and abuses in the area of search and online advertising, rather than the level of transparency in its information collection. Given Google’s huge and growing power throughout the online and mobile industries, though, this issue must be addressed, whether by Google itself or through outside investigation and enforcement. Even while Google

---

promotes its Project Glass\textsuperscript{23} and Google Goggles\textsuperscript{24} (both powerful information gathering tools), the company itself becomes less and less transparent, especially when it comes to privacy.