Privacy by Design and User Interfaces:

Emerging Design Criteria – Keep it User-Centric

June 2012

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Justin B. Weiss, J.D.
Senior Director,
International Privacy & Policy, Yahoo!

Acknowledgements

We gratefully acknowledge the work of Fred Carter, Senior Policy & Technology Advisor, Office of the Information and Privacy Commissioner of Ontario, Canada, in the preparation of this paper. We would also like to thank Illana Westerman, CEO and Co-Founder, Create With Context and Ms. Sandra Kahale for their helpful support and input on this project.

Information and Privacy Commissioner
Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

TABLE OF CONTENTS

Privacy by Design and "User-centricity"

The notion of informational self-determination seems to be collapsing under the weight, diversity and volume of "Big Data" processing in the modern Information Era. Understood as an individual's ability to exercise a measure of control over the use of his or her personal information by others, it is the basis for many privacy laws, codes of practice, and articulations of Fair Information Practice principles – especially the individual participation principles of informed consent, access, and redress. Individual participation is also expressed as a key *Privacy by Design* Foundational Principle: "Respect for the User: Keep it User-centric."

Privacy by Design principles, when applied, seek to proactively embed privacy into the design specifications of information technologies, organizational practices, and networked system architectures, in order to achieve the strongest protection possible.[1] In October 2010, regulators from around the world unanimously passed *Privacy by Design*, an international standard, as "an essential component of fundamental privacy protection," and committed to promote adoption of *PbD* principles in legislation, privacy policies, and as part of an organization's default mode of operation.[2] Since that time, diverse privacy regimes have taken up the call to endorse *Privacy by Design,* in either prospective legislation[3] or as a statement of best practice.[4]

The concept of "user-centricity" has evolved into two sometimes contradictory meanings in networked or online environments. For privacy types, it contemplates a right of control by an individual over his or her personal information when online, usually with the help of technology. For most system designers, it describes an information and communications system built with individual users in mind, and which anticipates and addresses users' privacy interests, risks and needs. One view is libertarian (informational self-determination), the other is somewhat paternalistic. Both views are valid, but must be qualified in an information age.

Privacy by Design embraces both understandings of user-centricity. Information technologies, processes and infrastructures must be designed not just *for* individual users, but also structured *by* them. Users are rarely, if ever, involved in every design decision or transaction involving their personal information, but they are nonetheless in an unprecedented position today to exercise a measure of meaningful control over those designs and transactions, as well as the disposition and use of their personal information by others.

As with the other principles of Fair Information Practices and *Privacy by Design*, *Respect for User Privacy* is not a stand-alone principle. It must be supported by the remaining Principles (*e.g.,* on transparency, security safeguards, default settings,

1 For extensive resources on *PbD*, visit www.PrivacyByDesign.ca.

2 International Conference of Privacy and Data Protection Commissioners. *Privacy by Design Resolution*, adopted at Jerusalem, Israel, October 27–29, 2010.

3 See, *e.g.,* Proposed Article 23 of the European Commission's proposed Data Protection Regulation for the private sector. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

4 See U.S. Federal Trade Commission Report: *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers* (2012), available at www.ftc.gov/opa/2012/03/privacyframework.shtm.

embedding privacy, and achieving positive-sum results). Good product and business process designs are needed to empower users to achieve strong privacy. Effective user interfaces are critical to good design and operation.

General user interface (UI) or user experience (UX) design ("UID/UXD") theory and evaluation criteria continue to evolve with 21st century technologies. The application of UI/UX design principles to the online environment and user privacy experience represents a subset of a much larger field of inquiry.

Context matters greatly in how design principles and criteria are applied. Legal requirements, project domain and scope, objectives to be achieved, and the nature, volume and sensitivity of the personal data processing involved will all vary in influence, along with the extent of user participation. Context must inform sound decision-making, and must therefore be the cornerstone of sound design.

In the online privacy realm, considerable research has been carried out questioning the relative effectiveness of traditional privacy policies and notices, as well as the unavailability to users of effective privacy options, preferences, tools and other controls.[5]

Interestingly, and despite some assumptions to the contrary, the same UI/UX design principles that translate into more effective and "successful" participation rates for, say, a promotional campaign or online contest, do not necessarily support privacy objectives. Adaptation to a privacy context requires taking a principled approach, executing judgement, and considering some form of metrics.

5 See for example:

- Michelle Madejski, Maritza Johnson and Steven Bellovin, *The Failure of Online Social Network Privacy Settings* (July 2011). http://bit.ly/MlkhFT;
- Pedro G. Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, and Yang Wang, *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising* (Oct 2011). www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html;
- Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, Lorrie Faith Cranor, *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach* (Jan 2010). http://bit.ly/NK34sQ;
- Nathaniel S. Good, Jens Grossklags, Deirdre K. Mulligan, & Joseph A. Konstan, *Noticing Notice: A Large-Scale Experiment on the Timing of Software License Agreements*, in PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 607, 615 (2007);
- Jens Grossklags & Nathan Good, *Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers*, in FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 341–55 (Sven Dietrich and Rachna Dhamija eds., 2007);
- U.S. Federal Trade Commission Report: *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers* (2012), op. cit.;
- TRUSTe, *Mobile Privacy: A User's Perspective* (April 2011). www.truste.com/why_TRUSTe_privacy_services/harris-mobile-survey/;
- Mary Madden, *Privacy management on social media sites* (February 2012). http://pewinternet.org/Reports/2012/Privacy-management-on-social-media/Main-findings.aspx.

Online Privacy and User Interface Design / User Experience

It has already been demonstrated that leveraging insights from various disciplines and functions inside and outside the organization, such as risk management, marketing, communications, information technology, and executive leadership, can yield powerful results when applied to a privacy program.[6]

In this paper, we suggest that the concepts associated with the discipline of User Interface Design also have much to offer that is relevant to the privacy community.[7]

For our purposes, *user interface* is the system by which people (users) interact with a machine. It includes hardware (physical) and software (logical) components. *Usability* is the term used to describe the degree to which the design of a particular user interface takes into account the human psychology and physiology of the users, and makes the process of using the system effective, efficient and satisfying. Usability is mainly a characteristic of the user interface, but is also associated with the functionalities of the product and the process to design it.

Further, it is useful to understand the notion of usability as including the extent to which a system/interface is usable for achieving objectives related to informational self-determination, as well as for communicating expectations and providing opportunities for feedback that help shape and clarify those expectations.

Current work on mobile and tablet technologies, with their small screens and unprecedented power, is throwing a spotlight on the importance of user interface design. An already well-established field,[8] UID/UXD is founded on rich concepts that can help privacy professionals as they approach the task of communicating their privacy programs into something that end-users can see and understand. These insights are the focus of the exploration at hand.

6 See www.ipc.on.ca for extensive resources on this theme, including:

- *Privacy by Design: From Policy to Practice* (Sept 2011);
- *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users* (Dec 2010);
- *Privacy Risk Management: Building privacy protection into a risk management framework to ensure that privacy risks are managed, by default* (April 2010, with the Ontario Lottery and Gaming Corporation);
- *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices* (Nov 2009, with Center for Information Policy Leadership and Hewlett-Packard); and
- *Privacy and Boards of Directors: What You Don't Know* Can *Hurt You* (July 2007).

7 Related disciplines of User Experience Design, Interaction Design, Agile Software Development, Usage-Centered Design, etc. are equally relevant and share some of the same principles. Some are more technically-oriented than others.

8 Ideas about User Interface Design have been around since the early days of computer technology, and reflect ideas that predate those technologies. See, for example, Don Norman, *The Psychology of Everyday Things*, Harper-Collins (1988), Bruce Tognazzini, *Tog On Interface*, Addison-Wesley (1991), Brenda Laurel, *The Art of Human Computer Interface Design*, Addison-Wesley (1991). Now, as computer interfaces grow smaller and smaller, the importance of UID is arguably greater than ever before. For more information about UID see, for example, www.useit.com, www.uxmatters.com, and www.uxmag.com.

This paper attempts to adapt and ultimately commend general UID/UXD principles to those practitioners working to deliver effective online privacy notices and meaningful privacy options. In doing so, we hope to broaden the discussion about user interface design criteria that should be considered when applying *Privacy by Design* principles to information technologies and systems.

User Interface Design Ideas for Improving Privacy Experiences

From the outset, the very concept of user interface design leads us to focus on *Privacy by Design* Foundational Principle #7, "Respect for User Privacy: Keep it User-centric."

User interface designers know that style (user interface) can often make or break an application. Function (substance) is important, but the way in which that function is delivered is equally as important.[9] This thinking influenced, for example, some research into the usability (or lack thereof) of tools to limit online behavioral advertising, an issue that has proven challenging and remains highly relevant to the privacy community.[10]

UID/UXD encourages us to view the act of translating an organization's privacy program into a value that its consumers can see and understand as being about creating an effective user privacy *experience*. That experience will necessarily include not only the organization's privacy policy, but also consideration of how, when and where users can learn about the policy, other salient information about data practices in a given context, and how, when, and where they can make choices that reflect their privacy preferences.[11]

Some of these issues fall within the purview of UID/UXD. In September 2011, an industry consortium led by *Create with Context* and including Yahoo!, Visa, and the Future of Privacy Forum, released preliminary findings of a study that looked at privacy issues in the mobile space. The study explored a number of themes, including how UID/UXD choices can impact transparency and trust.[12]

9 See, for example, Scott W. Ambler, *User Interface Design Tips, Techniques, and Principles*. www.ambysoft.com/essays/userInterfaceDesign.html.

10 Pedro G. Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, and Yang Wang, *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising* (Oct 2011) at: www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf The study looked at 9 different tools and found that none of them allowed participants to effectively control tracking and behavioural advertising according to their personal preferences. The authors concluded that "although we recognize the efforts of the advertising industry, browser providers, and third-parties for contributing an assortment of tools to this ecosystem, we encourage a greater emphasis on *usability* moving forward." *Ibid.* at 20.

11 It could also include provisions that reflect the principle referred to in the Canadian Standard Association's Model Code for the Protection of Personal Information as "Challenging Compliance" but those are beyond the scope of this paper. See Schedule 1, *Personal Information Protection and Electronic Documents Act.* (Canada), http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-18.html#h-25.

12 Create with Context, *Designing for Trust: The Mobile Initiative Preliminary Findings*. (Sept 2011), p. 9. www.createwithcontext.com/insights-digital-trust-and-privacy.php.

While many aspects of UID/UXD are quite technical, the *Create with Context* study highlights some core UID/UXD principles that strike us as both relevant and accessible to lay persons, and also particularly useful to privacy professionals engaged in designing user privacy experiences.[13] These concepts include:

1. Context
2. Awareness
3. Discoverability
4. Comprehension

Of course, these concepts are not new, nor are they necessarily unique to the field of UID/UXD. But considering them from a UID/UXD perspective by extending them to the development of the user privacy experience can help focus our attention in fresh ways on issues that have a real impact on transparency and trust.

Thinking through these issues within any given organization will likely yield many possible options and approaches. These should be weighed in accordance with that organization's own objectives and requirements. Ultimately, the best solution is one that provides both the necessary functionality and a rich user experience, giving meaningful effect to the concept of informational self-determination and contributing to maintaining trust. Such a win-win outcome is the hallmark of a successful *PbD* implementation.

Indeed, models for creating increasingly effective privacy experiences for users are already starting to be developed, and useful examples of some key concepts already exist. We highlight some of these in the discussion below. These efforts have particular urgency and relevance in the context of mobile technologies, which deliver new privacy and communications challenges and throw existing ones into sharper relief.[14] The iterative design paradigm reinforces the opportunity to build on emerging best practices, learn from them, and improve upon them.

1. Context

When it comes to understanding and expressing privacy, informational self-determination, and user-centricity, context is King. Personal information that is appropriate to collect, use, and disclose in one context may be completely inappropriate, or at least comparatively less relevant, in other contexts, frustrating efforts to develop detailed yet universal rules for engineering privacy and trust into the user experiences with technologies, organizational processes, and networked information architectures.

13 *Ibid.*

14 Visit www.ipc.on.ca for analysis of privacy issues associated with mobile technologies, including: *Wi-Fi Positioning Systems: Beware of Unintended Consequences* (2011), *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users* (2010), and *Mobile Near Field Communications (NFC) "Tap 'n Go" – Keep it Secure & Private* (2011).

Designers of user interfaces and experiences who are steeped in the demands of mobile technologies are quick to remind us of the need to consider the context of *devices*. To begin, an essential component of user-centricity is making it easy for users to see and absorb messages by being sensitive to the limits and opportunities afforded by the devices they are using. Mobile screens are very small; users should not be forced to resize or scroll endlessly in order to read privacy messages, and exercise privacy choices and preferences.

There is, therefore, an emerging push toward very short, readable text that mobile users can easily understand without excess scrolling. Designing for mobile devices from the outset, rather than designing for desktops and laptops and then attempting to retrofit these solutions onto mobile, makes for good design. The "mobile first" mantra is gaining ground in industry, and among policy-makers.

While this is still an emerging field, and expertise in mobile design applications is growing, in certain instances, the most effective realization of privacy functionality is one that recognizes that users may seek to perform similar functions across multiple devices. In this sense, a specific data processing activity can exist in multiple, concurrent device contexts. Ensuring that features have been designed to work for mobile devices, tablets and PCs is a core expectation of modern, effective design. Similarly, user privacy preferences set from one device should cascade across all related services and devices, even where the user interfaces for these may, by necessity, change.[15]

Context must include not only considerations of platform or device, but also the specific context surrounding particular instances of the collection, use, and disclosure of personal information. *Create with Context* cites an example of taking a photograph with an Android smartphone and having it appear automatically within Google+. Although it may be clear to the user that the photo is not posted publicly, it nonetheless makes them nervous to see it on that screen, which raises concerns about the potential for data leakage.[16] In anticipating and shaping user privacy experiences, privacy professionals should be sensitive to these kinds of issues, and offer appropriate notices and/or default settings to mitigate risk of unwanted surprise.

As practitioners begin to work more deeply from a user-centric perspective, it becomes clear that they should not only provide context for why the requested personal information is needed, but also provide their value proposition to the user.[17] So, for example, an application that wants to use location data may ask for permission in the context of a pop-up window that explains how the data will be used to deliver relevant content to the user. In addition to demonstrating value to the user, this approach has the benefit of improved transparency, and is consequently preferable from a privacy perspective over a simple request for permission delivered without context.

15 See, for example, Yahoo!'s announcement that it would support a Do Not Track signal globally, across platforms and devices, where Mozilla's Firefox sends it in the header. Press Release (March 29, 2012) at http://yhoo.client.shareholder.com/releasedetail.cfm?ReleaseID=660277.

16 Create with Context, *Designing for Trust: The Mobile Initiative Preliminary Findings*. (Sept 2011), p. 43.

17 *Ibid.*, p. 44.

2. Awareness

From a UID/UXD perspective, awareness is about whether a user knows that something exists. Clearly, the work of a privacy professional will be for nought without appropriate focus on ensuring that consumers know that privacy policies exist, and are aware of opportunities to exercise choice, and set their privacy preferences.

Here, timing, placement and form are quite influential. It is a common practice now, particularly for Web-based services, to require consent on sweeping privacy notices and terms of service at the outset of service offerings, when the context and meaning of these notices may as yet be quite unclear to the user. While we recognize that such requirements are often driven by law, reflecting a commitment to completeness and accuracy, design teams focused on user trust have realized that interactive material offered at the *time*, in the *place* and in the *manner* that is meaningful for users as they engage online is an important and useful component of maximizing the value of privacy programs and making such value visible to users.

We are starting to see better use of the time, place and manner component of privacy design in the context of information sharing in social networks. The notion is to offer users the opportunity to make privacy choices in the moment, when they are taking an action that involves their personal information. This kind of in-process communication clarifies the range of effective choice, and the implications of each choice.

One helpful example of this arises in the context of *Yahoo!'s Answers* product, which presents a privacy reminder screen to users prior to a public posting to evidence how a user's image would appear, and what name would be associated with the posting, prior to each publication. The defaults and settings are modifiable on a granular basis, which reinforces the specific awareness of the privacy consequences of his or her act each time there is a public sharing of information or content.[18] This exists as a supplemental overlay that relies on context to add meaning to decisions that may have already been established in other experiences, or under the general terms of the privacy policy.

Thinking like a user in designing privacy experiences will also raise questions about how long a permission remains in place, once it has been granted. *Create with Context* found that consumers were generally unsure, for example, whether they were agreeing to provide location information only one time, or continuously. Importantly, they did not think that location information was available to applications that were not running, although this understanding was, in fact, false. It is essential that the language used to explain value propositions and obtain permissions be clear and concise, without assuming that the user has intimate background knowledge of how an application or function works.

Awareness can also be supported with design choices that highlight the most essential information. An important consideration in approaching such design exercises is whether the focus is on information (explaining privacy policies) or on action (enabling users to make privacy choices).

18 See, *e.g., Ask a question* user flow in Yahoo! Canada Answers at http://ca.answers.yahoo.com/.

3. Discoverability

Informed by privacy considerations, the UID/UXD concept of discoverability includes a broad range of design considerations that impact the ease with which consumers can find pertinent privacy policies and adjust privacy settings.

Both *Privacy by Design* and user interface/experience design are concerned with architecture. Considering them together helps to highlight the aspects of information architecture that shape the user interface with privacy.

In the mobile context, for example, requiring too much scrolling or tapping frustrates users trying to access information and/or options. The same can be true of unfamiliar or inconsistent icons.

There are design choices to be made regarding whether privacy and/or account settings are accessible from each page (for example, in the form of an icon at the top or bottom of the page). Providing access to the same settings in multiple locations can be useful or confusing, depending on the approach and whether the same or different options are offered based on where the user accessed the settings.[19]

Design of clear navigation aids and interactive privacy notices is critical for ensuring discoverability. Users who become disoriented and lost on a site are compromised in their ability to understand applicable policies and options, and to exercise informed privacy choices. Jump links, for example, can help orient and empower users who access longer Web pages and documents. Signposting through documents to help with wayfinding, supplemented by action-oriented choices where appropriate, is a best practice for lengthy mandatory legal or privacy text.

Finally, drawing on concepts already used in general Web design to call attention to advertising or important content, manipulating colors or creating dedicated call-out boxes can help draw users' attention to important privacy-related updates relating to changes in policy, new policies or other messages that may be useful for users, particularly those that tend to rely on the transparency uniquely afforded by the comprehensive, complete privacy policies that are a cornerstone of business' accountability to the public.

Privacy professionals should work closely with designers and UID/UXD professionals to emphasize effective engagement and empowerment of users in the privacy interface. They should also be on guard for the ways in which organizational silos may express themselves in a manner that may impede the user experience by, for example, dispersing information about privacy practices to several places, such as Terms of Service, account settings, and system preferences without workable navigation between them.

19 *Ibid,*, p. 50.

4. Comprehension

A usability perspective on comprehension reminds us of the need to consider whether users understand what privacy policies and privacy settings actually mean.

Lengthy, legalistic privacy policies tend to discourage all but the most determined users. Taking this issue seriously leads us to explore alternative ways of communicating essential privacy information to users, and to enable them to make truly informed consent and other privacy decisions.

Another possible approach is using layered or "tiered" notices, which deliver short "just-in-time" subsets of policy information to aid users in making decisions, and allow users to choose topics of interest to them through simple navigation and to drill down further on specific areas and issues for more information and options.[20]

One way to implement this layering concept is to move away from relying solely on a singular privacy policy and move toward the concept of a Privacy Center, as Yahoo!, Google, and others have done.

Yahoo!'s Privacy Center,[21] for example, pulls together information about Yahoo!'s privacy policies from across its different services and product lines. It provides a one-stop shop for Yahoo! users to learn about the company's practices, edit their settings, and better understand how the information they share with, and through Yahoo! is used to shape their experience on its sites.

In the Privacy Center's home page design there is a strong focus on the role of *navigation*. Buttons dedicated to Products, Topics, Tools and Help frame the users' expectations and understanding about how to engage with the inevitably large volume of information and resources made available — information that would be far too much for any user to consume in one go, especially when "on the go."

Using the top navigation bar, users can also access Privacy Tools. Here, they can edit their profiles, set privacy preferences, opt-out of ad matching, and change their marketing preferences. Pooling these functions together in one place makes it easy for users to understand what their options are, and set them in ways that truly reflect their preferences.

Beyond avoiding legalese where possible, there is much that can be done to improve user comprehension of privacy practices. Terminology is tricky but important — writers cannot always assume that terms such as "third party," or "current location" will be clear to users, or understood by users across jurisdictions in the same way. Plain language is essential. Consistent use of icons can also be useful to introduce or communicate a new concept, when paired with appropriate education.

20 See, for example, The Center for Information Policy Leadership, *Ten steps to develop a multi-layered privacy notice.* (2007) www.informationpolicycentre.com/projects_archives/. Travis Pinnick's piece on Layered Policy Design for the TRUSTe Blog also offers some interesting insights. www.truste.com/blog/2011/05/20/layered-policy-and-short-notice-design/.

21 See http://info.yahoo.com/privacy/us/yahoo/details.html.

Research into the usability of tools to limit online behavioral advertising offers insight in this regard. In a study that assessed nine tools aimed at limiting online behavioral advertising, it was found that "[o]verall, [the] tools were ineffective at communicating their purpose and guiding users to properly configure them… [They] tended to present information at a level that is either too simplistic to inform a user's decision or too technical to be understood."[22] Language that may be clear to those working in the field cannot be assumed to be clear to the general public, as the present study bore out. Nevertheless, it is quite clear that the obstacles to comprehension presented by "oversimplification" contrasted with those presented by complexity as a byproduct of comprehensiveness and accuracy are at the heart of tensions in the privacy disclosure space. The iterative process of good design may also help yield an improvement of approach to text-based disclosures, relying on studies of their comparative efficacy to inform users in a meaningful way.

Summary and Conclusions

Considering the user — or, in the language of *PbD*, being user-centric — fundamentally means anticipating users' interests and capabilities, making it easy for them to interact with a given system, to understand the essential privacy-related processes, their applicability and relevance and to make effective use of available options to express one's privacy preferences and customize one's online experience. Failing to consider the user can have the catastrophic effect of coming across as being not only thoughtless, but also potentially deceptive. Clearly, this can have serious consequences for maintaining trust, especially in online applications whose success is built on consumer confidence. Just as it is highly advisable to proactively design privacy in from the outset, it is equally advisable to design the user's' perspective in from the outset, when creating privacy experiences.

Usability considerations encourage us to pay particular attention to consolidating privacy information into a single, intuitive place, presenting that information to users in a manner that is context-sensitive, and associating privacy controls with that information (e.g. embedding links to settings within the privacy policy, rather than making the user try to find them elsewhere), and using clear, concise and consistent terms to describe practices and value propositions.

Another aspect of user-centricity is accounting for who the user is, wherever possible, and designing and developing front and back-end systems that are appropriate to that user. When dealing with young users or children, for example, it may be appropriate for privacy design teams to adapt content or set defaults more restrictively, protecting privacy more aggressively in the default setting.[23]

22 Pedro G. Leon et al, *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*. p 4.

23 We recognize that the very act of "knowing" who precisely a user may be itself implicates and presumes a certain level of privacy impact, insofar as authenticated experiences are the privacy vehicle for Web companies to "know" their users. While this concept may not be universally applicable to anonymous Web surfing experiences, it is nevertheless an interesting reminder that companies are called on to design somewhat unique, adapted experiences, often centering on use. For interesting examples of "gaming" as a vehicle to instil privacy understanding into youth audiences, see Zynga's PrivacyVille (http://company.zynga.com/about/privacy-center/privacyville) and Yahoo!'s Maktoob Oasis (http://esafe.yahoo.com/index.php?lang=en).

Designing effective privacy notices and empowering user options will always remain an evolving work-in-progress. Challenges remain, chief among which are to establish consensus standards and best practices, and develop metrics for assessing the effectiveness of these user design criteria. This is the continuation of a design conversation for some, while it is a call to action for others.

The design principles we highlight in this paper are among those that we hope will increasingly be recognized in multiple contexts — in both corporate and public sectors alike.[24] We hope to encourage deeper investment by companies into the user design space, which will also contribute to a deepening evidence base that the privacy and policy community can draw upon in future *Privacy by Design* work.

24 We note, for example, the encouraging sign that this field is gaining in importance for the privacy community, based on its specific treatment on the agenda of the U.S. Federal Trade Commission's recent 30 May 2012 public workshop, *In Short: Advertising and Privacy Disclosures in a Digital World*, for which a comment period is currently open. www.ftc.gov/bcp/workshops/inshort/index.shtml.

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: (416) 326-3333
Fax: (416) 325-9195
Email: info@ipc.on.ca

Yahoo! Inc.
701 First Avenue
Sunnyvale, CA 94089
U.S.A.
Telephone: (408) 349-3300
Fax: (408) 349-3301
Website: www.yahoo.com | http://ca.yahoo.com/

June 2012

Privacy by Design: www.privacybydesign.ca

YAHOO!®