Date: 29-11-2013

In response to the ICO's Call for Comments for Privacy Notice Code of Practice

Date: 29-11-2013

We are writing this on behalf of the Open Notice community (and the Information sharing Work Group at the Kantara Initiative). We work with and are comprised of several organizations and projects that are working to evolve online privacy notices and terms-of-service infrastructure at Kantara. The Kantara Initiative is a non-profit professional association dedicated to advancing technical and legal innovation related to digital identity management.

Several recommendations for best practice have already come out of our work which will help inform the ICO's revised Privacy Notices Code of Practice.

We have noticed that this code of practices puts a tremendous onus on organisations to "make people understand" and this limits the meaning that this has for people.

There are many known issues with use of privacy policy notices that the new code of practice could consider including. We hope that future guidance allows for more proportional use of policy notice and preferences for people to better control the use of personal information.

Issues of fairness identified that should be considered:

- Companies range in size and resource and some would find it a great expense to have suitable notice for managing services with third parties across jurisdictions. E.g. Using Safe Harbour.
- People are unduly burdened with the responsibility of knowing all the policies of every service independently and this would costs people 76 work days a year to just read privacy policies personally (Aleecia M. McDonald and Lorrie Faith Cranor).
- People are unable to manage policy preferences easily post consent without logging in to every service or writing a letter
- Standard access rights are custom for each organisations who have the cost burden of providing infrastructure for managing personal information preferences and requests.
- People often have to deal with multiple policies when engaging in any transaction online not just one policy
- Organisations have different notice and consent rules depending on the jurisdiction and type of personal information involved

- There are currently limited ways for people to compare policies and check and see if their data is in fact used the way as proscribed in policy as suggested in the conclusion of the code.

Suggestions

In the call for comments we noticed that the ICO's code is based on fairness:

The current code mentions that Fairness has two main elements

1. Using information in a way that people would reasonably expect and in a way that is fair.
2. Ensuring people know how their information will be used, for example by providing a privacy notice or publishing it on your website.

A third element should be considered

3. Privacy policies should be as open as possible to encourage people to manage their own information and preferences.

The current code mentions the importance of keeping the notice up to date, but does not recommend any means to inform affected individuals about updates and changes to privacy practices. Privacy Notices are not yet open.

The Format of Privacy Policies

The layered approach covered on page 17 encourages a more open and responsive approach to preference management. This coincides with other efforts like the National Telecommunication and Information Administration short notices code of practice, which aim to prescribe layer notices for mobile.

Page 12 of the current code states that 'it's a lot easier to actively communicate a privacy notice in an online context than in a 'bricks and mortar' one. Advocating for the adoption digital ways of providing policy would be appreciated. Supporting the adoption of common identifiers and policy discovery practices is very high on various agendas that we are working with. Technically keeping a record or permanent link to governing policies and personal preferences is an area of the personal data ecosystem that is rapidly developing.

At present, several third parties in the Open Notice community provide services by recording/scraping website policies and sites. A great example is that of TOS;Dr (Terms Of Service Did Not Read), Ghostery and Mozilla's own browser plugin, Lightbeam. Many projects range from tracking cookies, track terms of service and tracking privacy policies, all all aim to help people understand and better use policy in more meaningful ways.

Visibility of Privacy Policy
Privacy notices on websites can be more or less visible. Organisations should follow best practices by providing a consistent, legible URI to the notice, and link to it in a standard, prominent place on the website.

Projects like Common Terms and IusOnsDemand help companies codify their information to provide layered notices. Emerging best practices for preferences should also be encouraged, projects like Customer Commons and the Customer's Voice are working to help companies find low cost ways for people to engage more actively. The URI or web address. should be concise and should not change or break. For guidance on emerging best practice for URI's, see http://warpspire.com/posts/url-design/ or http://www.w3.org/TR/cooluris/, this area is about to become much more important. Services like these I ensure that individuals who read the privacy policy and bookmark it for reference will be able to reliably return to it at a later date. It also means third-party tools which help individuals understand and manage privacy policies can reliably access the policies for assessment in the future.

Finding a Balance
The ICO has indicated that:

"We're keen to get the balance right between clear, general guidance and making sure the guidance works for new technologies."

Using Policy Post Consent
Page 10, consent raises important recommendations on best practices for obtaining consent. However it is currently silent on providing options and information related to withdrawing or managing consent. When a privacy policy involves asking for consent, opt-in or opt-out from the individual, a helpful best practice would be to provide a 'consent receipt' to the user. This would provide a record to the individual about what they have agreed to and when. It also helps establish the state of the policy at the time at which the individual consented to help people with vendor relationship management. Individuals can maintain a log of their consent

receipts, aided by their web browsers or other third party services. These receipts could be useful to make web experience more responsive. If also analysed and reviewed they inform individuals who may wish to change sharing preferences and even withdraw their consent at a later date or in context.

Page 13 of the code indicates when to actively communicate privacy notice. We recommend that publishing policies on the internet be a recommended practice.

Machine Readable Privacy Policy
While no widely-adopted standard for machine-readable privacy policies exists at the time of writing, a number of organisations are involved in standard-setting activity for this purpose.

Common Terms is a project which helps companies break their notices down into layers, the consistent ability to discover policy and its changes is very important for projects to provide value.

Proactive organisations designing or updating their privacy policies should stay informed of developments in this area and adopt best practices if and when they become established. The context of the notice should be made clear, i.e. which activities on which platforms, services or parts of the website are covered by the policy.What the jurisdiction is of the policy provider, if sensitive data is used, and a way to easily manage these in the future.

Sharing Information
“Sharing Information”, found on page 14, is one of the most difficult areas to negotiate in privacy, notice and consent. Keeping a an active list of sharing practices is a difficult task. An alternative would be to encourage people to manage their own preferences. For example, Do Not Track is permission that people set at the browser which website can use to make policy notices more responsive.

In Summary
The conclusion of the code of practice on page 15 indicates that, if there is a difference, (between the purpose people were told when providing personal information and the organization's intended use) people should be informed. As policies are not yet found in a common locations and in a machine readable manner online this is a challenge we hope this code will help address.

Date: 29-11-2013

Best Regards,

Open Notice & The Kantara: Information Sharing Work Group

Coordinators
Mark Lizar
Reuben BIns
Iain Henderson
Par Lannero
Hugo Roy
Mary Hodder
Valentino Sparta

Comments