Can Semantic Web Technology Help Implement a Right to Be Forgotten

Kieron O’Hara
Web and Internet Science Group
Electronics and Computer Science
University of Southampton
Highfield
Southampton SO17 1BJ
United Kingdom
kmo@ecs.soton.ac.uk

During the revision of the EU’s data protection directive, attention has focused on a ‘right to be forgotten’. Though the discussion has been largely confined to the legal profession, and has been overlooked by technologists, it does raise technical issues – UK minister Ed Vaizey, and the UK’s Information Commissioner’s Office have pointed out that rights are only meaningful when they can be enforced and implemented (Out-law.com 2011, ICO 2011). In this paper, I look at how such a right might be interpreted and whether it could be enforced using the specific technology of the Semantic Web or the Linked Data Web.

Access control on the Semantic Web
The Semantic Web suite of technologies and standards aims to progress the Web from a Web of documents to a Web that directly links data, facilitating automated machine processing of information (Shadbolt et al 2006). The Linked Data Web, linking data using Web standards (specifically URIs and the knowledge representation language RDF) without the full panoply of Semantic Web standards has also been gaining traction recently (http://linkeddata.org/). The aim of both visions is to allow principled linking of data across the Web, facilitating serendipitous reuse in unforeseen contexts.

Currently, the Semantic Web and the Linked Data Web approach access control via licences and waivers. In many cases, those who wish to gain the benefits of linking are keen for their data to be used and linked, and so are happy to invite access. Copyrightable content can be governed by Creative Commons licences, requiring the addition of a single RDF triple to the metadata. With other types of data, controllers use waivers, and for that purpose a waiver vocabulary, http://vocab.org/waiver/terms/.html, has been created.

These waivers and liberal interpretations of copyright are a long way from a genuine right to be forgotten, involving as they do relinquishing rather than re-establishing control over data. Indeed, the driving ideological assumption behind the Semantic Web has been the value of data sharing and amalgamation (a legacy of its scientific roots, and of the fact that data-crunching sciences are prominent early adopters). Meanwhile, data protection has generally been neglected. In the major textbook on linked data (Heath & Bizer 2011), the term ‘data protection’ does not appear at all. As the technology develops, data protection will need to be bolted on, in which case (as Lilian Edwards remarked to me, somewhat sardonically) “so much for privacy by design.”
O’Hara, Can Semantic Web Technology Help Implement a Right to be Forgotten?

The right to be forgotten

The scope of the right to be forgotten was outlined by the European Commission in a paper to the European Parliament (European Commission 2010), as:

the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. This is the case, for example, when processing is based on the person’s consent and when he or she withdraws consent or when the storage period has expired.

If we take the example as a paradigm, this doesn’t seem unreasonable; if the processing can only take place with the subject’s consent, then he or she might expect to be able to withdraw that consent. More recent comments (e.g. Pop 2011) seem to suggest that the Commission is currently minded to interpret the right in a way that does not overly extend existing rules.

In that case, the proposal resembles sophisticated consent management. In the UK, there is already interesting work going on in this space, in projects such as Visualisation and Other Methods of Expression (VOME – http://www.vome.org.uk/), which is investigating how ordinary computer users interpret, express and visualise information privacy and consent, and Ensuring Consent and Revocation (ENCORE – http://www.encore-project.info/), a more technical project developing architectures for empowering data subjects to express, manage and enforce their consent decisions. Flexible consent management is certainly difficult, but hardly merits inflated rhetoric about a new right; the products of VOME and ENCORE and their successors will probably be used largely by data controllers to maintain good relations with the subjects of their data. In particular, the questions of enforcement raised by Vaizey and the ICO are not addressed by such projects.

The Policy-Aware Web

In Semantic Web and Linked Data Web research, the most relevant strand is the so-called Policy-Aware Web (Weitzner et al, 2005), in which rule-based policy languages and theorem provers are used together with HTTP to provide a scalable protocol for exchanging and applying privacy preferences. Preferences are encoded as policies and associated with the dataset as metadata. A policy might express restrictions such as “you may share these data only with my consent” or “you may only share these data with those who are within two nodes of me in a Friend-of-a-Friend (FOAF) graph”.

This would allow the development of discretionary access control using Semantic Web methods. Theorem provers could establish whether data usage is in accordance with policies. The main thrust of research to date has been in conditional access restriction, but one could imagine introducing time stamps, to restrict access beyond some particular time $t_1$. This could then constitute something like an automatically-triggered ‘right to be forgotten’, as suggested by Viktor Mayer-Schönberger (2009). One could also imagine conditional policies, possibly including input from data subjects, implementing a flexible consent management system.

Here is an example from (Kolovski et al 2005), expressed in the language REIN, a variant of N3 (a human-readable version of RDF) designed to represent rules. The example policy in English is:

An agent can access our information if (i) it is affiliated with the MIND lab institution, and (ii) the information is requested on a workday. Furthermore, one
meets (i) just in case one’s provided email address is a MIND lab email address, which have a specific form.

The policy is then written as follows in REIN.

R1: Conditions for being an authorized agent

\[\begin{align*}
?agent & \text{policyP:hasMINDAcct ?email.} \\
?agent & \text{policyP:requestsAccess ?request.} \\
?request & \text{policyP:requestTime ?time.} \\
?time & \text{a policyP:validRequestTime.} \\
\Rightarrow & \{?agent \text{ a policyP:authorizedAgent.}\}
\end{align*}\]

R2 : Conditions for having the proper email credentials

\[\begin{align*}
?agent & \text{foaf:mbox ?email.} \\
?email & \text{string:matches ",.*?@mindlab.umd.edu\$".} \\
\Rightarrow & \{?agent \text{ policyP:hasMINDAcct ?email}.\}
\end{align*}\]

R3 : Conditions for the times when a request can be processed

\[\begin{align*}
?agent & \text{policyP:requestsAccess ?request.} \\
?agent & \text{policyP:requestTime ?time.} \\
"" & \text{time:localTime ?localTime.} \\
?localTime & \text{time:dayOfWeek ?day.} \\
?day & \text{math:greaterThan "0".} \\
?day & \text{math:lessThan "6".} \\
\Rightarrow & \{?\text{time a policyP:validRequestTime.}\}
\end{align*}\]

Even given that this is human-readable, it is a moot point how easy or routine it would be for a human to express or understand such policies, or how flexible they could be in a real-world context. For instance, how would the above cope when someone needed access out-of-hours, or insisted on using a non-standard email address? The policy itself could not, but in the absence of any enforcement method, management might be able to work around the code. Yet the need for a workaround is hardly ideal (it is only fair to the authors to point out that this is a simplified example, and the priority of researchers on Web standards is to establish systems that work at the Web scale, before addressing usability).

We should remain alive to the limitations of this approach. It is aspirational, allowing the data controller to express preferences about how the data should be reused. This would be an advance, though only one step toward genuine accountability for information use; no practicable enforcement mechanism is on the horizon. Furthermore, it is a tool for controllers, not data subjects (who should be the beneficiaries of a right to be forgotten); subjects’ preferences would be written into (or excluded from) a policy at the controller’s discretion.

**Beyond consent management**

If the right to be forgotten goes beyond consent management, and becomes the more powerful idea of deletion of content across the Web, then the Semantic Web will be stretched to help. The notion of the Web as a common and public information space is designed pretty solidly into it. Although that ideal can be undermined by walled gardens such as Facebook, and bottlenecks such as bit.ly (Zittrain 2008), even then data subjects’ writ rarely goes beyond walled-off areas they themselves control.
Even assuming that we can address the usual uncertainties about a right to be forgotten (How do we trace uses of our data? How do we deal with different jurisdictions, especially outside the OECD, or in the US with its fetishized First Amendment?), and that we produce a practicable definition of ‘delete’ (May the data be archived? Aggregated? Published using robots.txt? Is hiding from search engines enough?), Semantic Web research points up further problems which will inevitably crop up. In particular, one of the most serious is coreference resolution: how do we establish that two instances of the same name refer to the same person, or alternatively how do we reliably and scalably find all the names of a particular individual (not only variants such as ‘Kieron O’Hara’ and ‘O’Hara, K.’ but also misspellings and deliberate renaming)? This is a massive problem in the linked data world, even on the relatively small scale of current practice (e.g. Glaser et al 2009). The related issue of tracing provenance poses similar problems.

Discussion: do we even want a technical solution?

The example quoted earlier from shows how difficult it is to write flexibility into policies. And yet flexibility must surely be a prerequisite of conditional access management; for instance, consider the differing restrictions placed on data about someone’s association with a particular crime depending on whether they are being sought by police, have been charged, are being tried, have been acquitted, have been convicted, their conviction is spent, they are being tried for another crime, they are seeking public office, or they are dead. Can we predict and express the complex social role of information in time stamps, or will the nuances resist encoding?

The social value of data – which the Linked Data Web and Semantic Web are intended to enhance – is contingent and inherently unpredictable, against which background any technical solution to the right to be forgotten will seem arbitrary (one blogger has likened it to ‘burning down the library every five years’). A vital mechanism in human and social memory is association; we find information not by inference, but by following links. This is why the Web is so powerful and why the Semantic Web holds such promise. Even if we ignore harms to individuals from removing access to data that someone wishes to be forgotten, the social harm of implementing a right to be forgotten must surely outweigh the sum of individual gains.

If there is to be an ambitious right to be forgotten, it must be a socio-legal construct, not a technical fix.

References


ICO (2011). The Future of Data Protection in the EU, Information Commissioner’s Office briefing note,
O’Hara, Can Semantic Web Technology Help Implement a Right to be Forgotten?


