Enabling Enterprise Privacy through Bi-Lateral Negotiation

Robert Thibadeau, Ph.D.
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
rht@cs.cmu.edu

Personal information privacy is a subject in constant tension along a number of interesting dimensions, but it should not be the subject of compromise. It is highly related to computer security in sharing this dichotomous attribute that should not be the subject of compromise, and it is highly related to digital rights management that similarly cannot afford compromise.

Comprehensive laws have the flaw that they are inherently compromises. They can act as default contracts, but people must have the flexibility to set contractual conditions that allows individuals and individual organizations to customize the defaults based on specific context.

An interesting case to illustrate this contextual sensitivity is in the distinction between “use” and “purpose” – what is being done and why. Contractual law, in the area of non-disclosure agreements, distinguishes use and purpose, and generally requires a statement of both. Privacy is no different as the semantics of P3P recognize. The use a company makes of personal information is only one facet of the privacy equation. There is also the question of why this use is made. The purpose helps us judge the use as a plausible use. Even though we may be concerned with the use, we can be comforted that there is a contract that explicitly states intent.

“Why” is a ugly term in formal languages, and certainly it has similar problems in legal instances, because it appeals to “reason,” “common sense,” and other things that we don’t really have a clue about formalizing. But it does permit forensic exposure. If the reason for analyzing medical records is to research new cures, then using the medical record access system as a way to judge employability is arguably a violation of the purpose, even if we write the use in a way that permits judgments of employment. This notion of exposure is what exists out of contract law in non-disclosure agreements. The government does not send prosecutors after violations of contracts, but it does establish the vehicles through which violations of contracts can be exposed, and justice sought and at least sometimes achieved.

If we consider law to be a framework for default contracts, then we can consider contracts as modifying law. In the United States, we may say there is no default notion of a “right to privacy” but in Europe there may be a default right to privacy. Contracts, however, may modify these defaults in ways permitted by these default laws. Furthermore, we may not have situations, such as “purpose,” where automated judgment or remediation is impossible. We may only have situations where exposure, or the threat of government sanctioned exposure, is the remediation.

The problem in the case of personal information privacy, as well as, by the way, computer security and digital rights management, is that events overcome us. There seems little doubt, for example, that a person who is relatively active on the Internet is the subject of many thousands of ‘privacy decisions’ a day because of all the mailing lists, past behaviors, and even his offline behaviors with service providers who digitize information about him. Pick a number. Say, 20,000 a day. No human can judge all these situations, and it may not be enough to have law controlling all of these. But let’s say that 90% are readily handled by default law. That still leaves 2,000 a day. Far more than is possible. So, let’s say 99% -- still, 200 contracts a day. Yet we know a single person’s ‘contract negotiation capability’ is more like a contract a month, let alone 200 contracts a day. When the use and purpose is “other” and a blank if filled in, how long does it take to make a reasoned judgment permissioning a use of personal information?

At CMU, we had proposed the notion of persona as a tactic that allows sub-classing contracts below the default contract level. A person simply selects the “Ted Turner” persona because it is close to what his preferences demand. But for a persona mechanism to work, the standards must enable persona that are fully capable of solving all the problems of establishing context aware contracts. Persona can make demands that no individual can make. A persona can represent hundreds of thousand of people who have stood together with respect to a consistent set of demands.

Persona mechanisms should be promoted to grow ‘in the wild.’ We should not, I believe, be stipulating a set of persona, but rather providing a fully capable Internet vehicle. This is where the role of enterprise privacy can play the strongest role, since it is a well recognized imperative that an enterprise, such as ‘an Amazon’, has its ‘privacy management’ (and also digital rights management) problem multiplied by the number of visitors a day. It may be OK for an enterprise to accept the rights and obligations demanded by a certain popular persona, perhaps even popular only within a community of use (such as medicine) while not accepting all possible persona that are in the wild. So, perhaps, the enterprise can handle 80% of the situations it encounters through defaults, we may be able to reach substantially all through persona. The remainder may be refused except at the default law level – a simple decision.

By “a fully capable vehicle” we must also consider contracts that bind, that permit exposure of injustice, and we must consider life-cyle issues such as successor arrangements and the like. It is imperative, I believe, that full automation be possible for negotiating and executing contracts. It may take great study and effort to develop persona, and relations among persona, but once these are established, they should act automatically and with certainty and determinism. An interesting role for P3P would be to look at mechanism but not necessarily at what the persona will eventually be.

Exposure has the same problem of numbers as the contracts themselves. If there are a million exposures of contract violations a day, no one will notice one. The “fully capable vehicle” must handle this problem as well.

The typical user of such a system would go fishing on the Internet for persona that he likes. He would acquire those persona, perhaps only four or five, perhaps many more. Later, as he interacts on the Internet, these would be invoked at appropriate times to negotiate on his behalf. The typical enterprise user of such a system would notice what persona are being offered to the enterprise and would develop policy regarding them. Presumably the system would support the development of optimum negotiation strategies. A "Default Law" persona would simply revert to local default law as long as jurisdiction is identified, or, perhaps, accepted. To be more concrete, here is one scenario:

1. A Persona triggering condition: A Persona may have built in triggering conditions, such as requestor type: "Medical," "Official Government," "Retail Online Sales." Presumably it would be possible to trigger more than one Persona, so…
2. Selected Persona may be ordered by the user or at least partially ordered and this may be requestor type specific ordering.
3. The Persona has certain 'template aspects' that associate personal information with specific variables in the Persona. This allows a Persona to be constructed with fine-grained control over the release of information. In keeping with this, a Persona should have a well-known way to fill out a form.
4. The elements of the Persona also include negotiation rules operating off the P3P semantics but these would also be extended. For example, there may be a recourse that specifies a public (and machine readable) complaint registry, through, perhaps, a registry of registries.
5. Complaints may be profiled. For example, they may be strengthened with "proof" such as cryptographic signing. The semantics may be extended to require a recourse process that first seeks recourse with the enterprise.
6. On the Enterprise side, persona should come with 'convenient handling' tools. Enterprises should be able to inspect the negotiating behavior of a persona in order to formulate strategies for quickly coming to an automated conclusion. At a first level, persona should have universal names, so a quick decision can be made "If this is the Ted Turner persona, accept it." Agreements should all have a universal form to the agreement. Perhaps the simplest is to name the persona and the enterprise accepting it.
7. In the vague category of "other" there should be a clear way to point to a registry where "other" values are offered up with definitions. Ideally, no persona and no policy will require a 'naked other' that requires human attention except in set-up. So an enterprise may publish its acceptable "other" values on some semantic dimensions, just as it may also offer up persona (e.g., "Amazon Shopper").
8. Persona should also have 'handling hooks.' These may include listing data service providers that can handle a persona's requirements if the Enterprise so chooses.

The idea of such a Persona mechanism is that the creator of a Persona is essentially a "Power User of our Internet privacy system" while the typical users of such Persona just establish trust relationships (I trust that Ted Turner's desire for medical privacy is good enough for me). Enterprise users can analyze such Persona in an automated way to determine conformance to Enterprise policy. (E.g., Persona Ted Turner's desire for medical privacy is acceptable for our online Pharmacy operation, else No.)

Providing the tools that will stimulate the production of such solutions is an aggressive goal, but I believe that this is an achievable goal if approached directly. The solution will happen because we are not trying to determine the terms of such contracts, but because we are providing the vehicles through which terms can be developed and constantly refined through use. The semantics of P3P will always be incomplete, but a stronger focus on a versatile mechanism, and then the appropriate 'registration authorities' for publishing aggregations, may yield a very interesting and important result.