Moving Forward from PETs to PETs ***Plus***: The Time for Change is Now

March 2009

Moving Forward from PETs to PETs ***Plus***: The Time for Change is Now

Traditional PETs

Privacy-Enhancing Technologies (PETs) refer to information and communication technologies (ICTs) that strengthen the protection of personal privacy in an information system by preventing the unnecessary or unlawful collection, use and disclosure of personal data, or by offering tools to enhance an individual's control over his/her personal data.

PETs were developed in the '90s with the goal of enlisting the support of technology to enhance privacy, rather than encroach upon it. But the time has come to move the bar forward. PETs alone may at times be found to be lacking, which is why we have evolved the term to "PETs *Plus*."

Since first coining the term "PETs" in 1995 with the Dutch Data Protection Authority, I have emphasized the need to incorporate the universal principles of Fair Information Practices (FIPs) directly into the design and operation of information processing technologies and systems as part of my "Privacy by Design" philosophy.

First codified by the OECD in 1980, FIPs come in a variety of flavours, including the E.U. Directive on Data Protection, Canada's CSA Privacy Code, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, the U.S. Safe Harbor Principles, and, most recently, the harmonized Global Privacy Standard, which I led with international Privacy and Data Protection Commissioners, in 2006.[1]

Despite minor differences, these FIPs all share the following fundamental common denominators:

- **Data minimization** – the collection, use, disclosure and retention of personally identifiable information should be minimized wherever, and to the fullest extent, possible;
- **User participation** – individuals should be empowered to play a participatory role and to exercise controls during the life cycle of their own personal data; and
- **Enhanced security** – the confidentiality, integrity and availability of personal data should be safeguarded, as appropriate to the sensitivity of the information.

1 Cavoukian, Ann, Ph.D., *Creation of a Global Privacy Standard* (November 8, 2006): **http://www.ipc.on.ca/images/Resources/gps.pdf**

Traditional PETs promote user participation and empowerment

PETs should ideally promote *all* of these meta-principles. For example, an organization's use of strong encryption technologies to secure detailed customer records against unauthorized access and use, while extremely valuable, in and of itself, speaks little to the data minimization and user participation requirements.

Traditional PETs contribute to the privacy ideals of informational self-determination, that is, an individual's ability to exercise a measure of control over the collection, use and disclosure of their personal information. Given the history associated with the early developments of PETs in the 1990s, namely growing concerns with online surveillance issues, this is not surprising. As a result, online PETs have been typically defined to perform the following functions:

- preventing unauthorized access to communications and stored files;
- automating the retrieval of information about data collectors' privacy practices and automating users' decision-making on the basis of these practices;
- preventing automated data capture through cookies, HTTP headers, web bugs, spyware, etc.;
- preventing communications from being linked to a specific individual;
- facilitating transactions that reveal minimal personal information; and
- filtering unwanted messages.

These are user-centric tools and functions. The list has not been significantly lengthened in over a decade, and strongly suggests that PETs are discrete technologies that put individuals in greater control of their own personally identifiable information.

But have unnecessary boundaries been placed upon PETs? Are they cryptographic primitives, software or hardware applications, components embedded in larger systems, or entire information systems? Should PETs be understood to include only technologies under the exclusive control of the individual, or is there room for a more expansive definition that includes greater infrastructure components? The door must be widened.

PETs *Plus*

In widening the door, I felt that the concept of PETs had to be expanded. PETs *Plus* represents the evolution of PETs by adding a "positive-sum" paradigm to ICT designs and uses. The result is that PETs *Plus* seeks to achieve goals in addition to those intended to protect the interests of the individual alone. That is, PETs *Plus* facilitates achieving the goals of other participants or stakeholders such as, for example, those of the system owner and operator, in a positive-sum, not zero-sum model. These may be the functional and operational objectives of the system (e.g., to transport and route electronic communications, to process a payment, or provide a service), or other security, surveillance, and anti-fraud detection goals.

Again, these additional goals do not come at the expense of the individual (zero-sum), but in *addition* (positive-sum).

PETs *Plus* recognize the importance of infrastructure

How can PETs *Plus* achieve other goals in addition to privacy? By abandoning the prevailing zero-sum model of privacy *vs.* other interests. Not only is the zero-sum approach doomed to failure, but it is also the least efficient model to employ. The starting point should be the recognition that virtually all PETs possess an infrastructure component, in order to perform to their optimal level. For example: take a traditional PET, such as a software utility that individuals can download and install onto their computers to securely encrypt their files and email messages. In order for it to function, users must trust the embedded encryption algorithms to do their magic – that the downloaded file will come from a reliable source and will be "clean" when installed. In order to securely communicate, other users must also have the same software program installed on their computers, and be able to connect, using appropriate infrastructures. To facilitate the exchange and lookup of (PKI) encryption keys, public key servers may need to be available, hosted by trusted parties, and so forth.

The same reliance upon infrastructure and other parties is also true for another quintessential PET, the Platform for Privacy Preferences (P3P), in which users can establish their machine-readable privacy preferences, which are then automatically matched against the privacy policies of participating websites visited. In order to have any privacy relevance or utility for the individual, P3P protocols must be supported "by the infrastructure."

Finally, it should be noted that anonymizing proxy servers or networks, which allow individuals to surf or communicate anonymously, pseudonymously, or in an otherwise untraceable manner, depend critically upon a trusted, enabling infrastructure. There may be some linked component that resides on a user's computer that is under that person's control, but the network is itself, the PET, and the user interface is just that – an interface.

PETs *Plus* recognize the importance of design and architecture

Do traditional stand-alone PETs, when built into the "infrastructure" suddenly stop functioning as a PET? In a word: No. For example, password managers, "cookie cutters" and spam filters are often held up as examples of PETs, because they are discrete tools that empower users and minimize the unwanted processing of sensitive data. But when these PETs are integrated into operating systems and browsers, do they necessarily lose their privacy-enhancing qualities? Is there a difference between a stand-alone password manager and the one offered by Firefox or Internet Explorer? Are spam filters that are installed and configured exclusively on one's home computer or client application any more of a PET than those installed and operating at the internet service provider infrastructure level?

I argue that no, PETs can be one or the other, or both. Either way, it is critically important to recognize that the infrastructure is often an essential component of PETs, and can sometimes even become the *entire* PET.

PETs *Plus* promote user confidence and trust

The (growing) importance of information architecture design and infrastructure has implications for user empowerment and control. Because the behaviour of infrastructure components is often beyond the direct access and control of individuals, a certain degree of reliance and trust is essential.[2] In the context of networked cloud computing and the exponential creation, use and disclosure of personally identifiable information by more and more actors, this reliance and trust must in turn grow. It does not mean that PETs are becoming less relevant. Quite the opposite: PETs must evolve in tandem, and make possible a new era of privacy confidence and trust… enter PETs *Plus*.

Take, for example, enterprise PETs or corporate PETs, meeting both the needs of the organization *and* protecting privacy. These are privacy-enhancing technologies that are deployed entirely within information architectures and systems owned and operated by organizations, rather than by individuals. "Enterprise" PETs can facilitate better organizational controls and privacy compliance for all uses of personal data, in a given system. The privacy practices of data minimization and improved security may be fully operationalized but, in place of individual participation, there is a growing focus on ensuring system transparency, consistency, and accountability. One example would be an enterprise privacy technology that attaches privacy policies directly to personal data and automatically tracks their usage, enforcing those policies across the entire enterprise, and beyond.

At this point, while the degree of user participation may diminish, privacy does not. It only takes a short step to recognize that PETs may be built directly into organizational infrastructures in such a way that privacy benefits may be achieved with minimal or no user participation.

In summary, these are examples of PETs *Plus* – when enterprises or "architectural" PETs achieve both privacy and enterprise functions in a positive-sum way, enabling privacy *and* system functionality.

2 How that trust is secured can vary enormously, e.g., open-source code, open competition and availability of alternatives, third-party testing and certification, warranties and guarantees, reputation, direct audit tools, etc. Indeed, one emerging class of PETs identified is transparency and audit tools that allow individuals to make better informed privacy decisions in their online and offline interactions.

Transformative Technologies

It gets even better: when PETs *Plus* are applied to traditionally privacy-invasive technologies, such as video surveillance systems – without any meaningful loss of functionality – these technologies can, in effect, be *transformed* into behaving like privacy-protective ones. This set of PETs *Plus* we call *Transformative Technologies*.

I have identified Transformative Technologies in the following traditionally "privacy-invasive" areas:

- Biometrics
- Radio-Frequency Identifiers (RFID)
- Video surveillance cameras
- Network tracing and monitoring
- Whole body imaging
- Online digital identities

Conclusion

PETs *Plus* are Privacy-Enhancing Technologies applied within a positive-sum, not zero-sum paradigm, often resulting in the creation of *Transformative Technologies*.

From a privacy perspective, all ICTs are essentially neutral. What matters are the choices made in their design and use – technologies may be designed to be privacy-invasive or privacy-enhancing. PETs embody fundamental privacy principles by minimizing personal data use, maximizing data security, and empowering individuals. The concept of Privacy by Design that I introduced in the '90s extended the concept of PETs to emphasize the need to embed privacy at the design stages of information technologies, architectures, and systems – all of which are often beyond the control of the individual. Organizations that embed privacy early on will benefit in a number of sustainable ways from the resulting privacy payoff.

Today, these messages are more relevant than ever, as we collectively face a world of ubiquitous data availability (in the words of Professor Fred Cate). Building upon my positive-sum approach to advancing privacy, I encourage the development of a new generation of PETs – PETs *Plus* – which can actually transform otherwise privacy-invasive technologies into privacy-protective ones, with little or no loss of functionality. This new breed of *Transformative Technologies* can also transform privacy problems into lasting privacy solutions – ensuring that privacy lives well into the future.