Security and privacy are often seen as opposite, irreconcilable goals. Privacy partisans and security sharks cling to rigid points of view, fighting each other in exhausting trench warfare. As a result, measures to increase our security seem to scorch our privacy, while privacy-enhancing technologies (PETs) do very little to address legitimate security concerns.

The concept of revocable privacy aims to bridge the two sides of the debate to break the status quo. Revocable privacy is a design principle (which includes the necessary toolbox) to build information systems that balance the needs of both security and privacy. The underlying objective is to design a system that guarantees the privacy of its users, unless a user violates a predefined rule. In that case, |I|>ersonal information might be released. Laws and regulations by themselves are insufficient; they can be changed or sidestepped later on. That is why the principle of ‘code as code’ is taken as the point of departure; the rules and regulations must be hard-wired into the architecture of the system itself.

This article introduces the concept of revocable privacy and shows that certain techniques to solve this important problem already exist.

Security versus privacy? Trench warfare
Homeland security is a political top priority. Whether it concerns fighting crime or terrorism, citizens demand that their government takes appropriate action. For example, it is hard to argue to the general public why producers of child pornography can go their way unhindered on the Internet. To combat terrorism and to stop cyber-crime much potentially privacy-sensitive information is useful. But where does it stop? When should privacy start to prevail?

Sometimes loosely defined as the ‘right to be let alone’, privacy has many dimensions. Technological developments, such as the invention of the computer and the rise of the Internet, have had profound implications on the privacy of citizens. It is important to realise that privacy is not only of personal value, but also a common societal good. It is a prerequisite for realising all of one’s own potential and for developing one’s own opinion without interference, which in turn contributes to the development and innovation of society as a whole.

Unfortunately security and privacy are seen as enemies of each other. It is thought – though without good grounds – that one cannot be achieved without sacrificing the other. This tension between security and privacy is felt in many areas of public policy-making. Examples include camera surveillance, systems for road-pricing, interconnecting national and international databases for law enforcement purposes, ID cards and their integration into national systems for identity management and eGovernment, and many more. For lack of alternatives – or sometimes for lack of understanding – more attention is paid to the security of the system in its development, under the mistaken assumption that a focus on privacy would be detrimental to security. Given the high political importance attached to security these days, this has resulted in approaches to increase societal safety that disregard the privacy of the citizen. Similarly, when designing PETs, no attention is paid to the quite reasonable request to also consider issues concerning the security of society. This is a highly undesirable state of affairs, both from a security and from a privacy point of view.

The need for a technical approach
The necessary mind-shift is to realise that legal or regulatory attempts to remedy the situation are inadequate. Rules and regulations may change over time, allowing for new ways to gather information about people after the fact. Such ‘function creep’ occurs frequently; it seems that, once the system, allows certain methods of collecting data in principle, sooner or later politicians or law enforcement agencies will ask for an extension of powers. The solution, therefore, must be found in limiting possibilities at the outset, through technical means, in the architecture and design of the system.

This line of reasoning follows the idea of ‘architecture is politics’ and ‘code is code’ of Prof. Lawrence Lessig (www.lessig.org) among others. By embedding the rules, procedures and regulations (the code of conduct) into the implementation (‘the code’) of the system, they can no longer be changed after the fact. Such a change would require a complete redesign (and re-implementation) of the system. To balance security and privacy needs and achieve a reasonable trade-off we are developing the technical concept of revocable privacy.

Revocable privacy
In essence, the idea of revocable privacy is to design systems in such a way that no personal information is collected, unless a user violates the (pre-established) terms of service. Only in that instance will the personal details, and when and how the terms were violated, be revealed. The data will only be revealed to authorised parties, of course, and the guarantees are technical rather than legal in nature. We define revocable privacy as follows:

“A system implements revocable privacy if a predefined rule has been violated”.

---

Jaap-Henk Hoepman

---

Example, it is hard to argue to the general
We distinguish two variants of revocable privacy.

- **Spread responsibility.** One or more trusted third parties verifies whether all conditions for releasing personal data have been met, and grants access (or releases the data) if this is the case.

- **Self-enforcing architecture.** The rules to release data are hard-coded into the architecture. If the rules are violated, the data is released automatically. If no rules are trespassed, no information can be obtained at all.

**Implementing revocable privacy**

Many of the techniques currently in use for revocable privacy are based on the use of trusted third parties. By spreading power over many such parties (using secret sharing techniques or similar), one can mitigate the likelihood of corruption or subversion. However, such systems are in essence still based on procedure; by changing the procedures and replacing the trusted parties, one can still change the rules of the game. We therefore believe that self-enforcing approaches to revocable privacy are the way forward.

The idea of revocable privacy is certainly not a new one; back in 1988 David Chaum proposed a scheme for off-line digital cash where double-spending a coin would reveal the identity of the owner of the coin. To achieve this, the protocol governing the spending of a coin uses a so-called ‘cut-and-choose’ technique.

**Spotting canvas cutters**

There are also other, more recent techniques that appear to be promising. One example is homomorphic cryptography, where the encryption $E(x)$ of $x$ and the encryption $E(y)$ of $y$ can be added to yield the encryption $E(x+y)$ of $x+y$. In other words, $E(x+y) = E(x) + E(y)$. Using these ideas, one can also implement threshold encryption, where a group of $N$ users encrypt a value using their own private key, in order to decrypt the value (using a single public key), one needs at least $T$ different encrypted values.

To see how threshold encryption can help achieve revocable privacy, consider the following real-life example. So called ‘canvas cutters’ are criminals who roam the parking places along highways and cut the canvas of trucks, looking for valuable content. To identify possible canvas cutters, one could set up ANPR (Automatic Number Plate Recognition) systems at the entrance of each parking space and search the resulting data stream for cars that enter multiple parking spaces along the same highway on a single day. Clearly this poses a privacy threat, as the data of all cars visiting a parking place are retained. One could choose to retain the data coming from a single ANPR system for only a couple of hours. But this is only a procedural measure. Another option is to encrypt all number plates recognised by each ANPR system immediately using a threshold encryption scheme, and only store these encrypted number plates. Setting the threshold at a suitable level, say 3, the authorities only retrieve number plates of cars that visited at least three parking spaces on a single day along the same stretch of highway. The advantage is that no useful information whatsoever is stored about any of the cars that were not registered at least three times.

**Conclusions**

Revocable privacy is a method of designing systems that could help to realise both security and privacy requirements when building information systems, thus bridging the gap between security sharks and privacy partisans. Techniques to implement revocable privacy already exist, although they are only applicable in specific cases. More general techniques need to be developed and a co-ordinated research effort on this topic is desirable. However, the underlying design principles to achieve revocable privacy are already deployable, using either general trusted third parties techniques or special purpose mechanisms.

Dr. Jaap-Henk Hoepman (jhh@cs.ru.nl) is a senior scientist on security and cryptography at TNO, an associate professor in pervasive security at the Radboud University Nijmegen, the chair of IFIP WG 11.2 on small system security and a member of ENISA’s Permanent Stakeholders’ Group.