From Panopticon to Fresnel, dispelling a False Sense of Security

Jon Crowcroft[1] and Ian Brown[2]

[1] The Computer Laboratory, University of Cambridge jon.crowcroft@cl.cam.ac.uk
[2] The Oxford Internet Institute, University of Oxford ian.brown@oii.ox.ac.ac.uk

Abstract. Sensor networks are typically purpose-built, designed to support a single running application. As the demand for applications that can harness the capabilities of a sensor-rich environment increases, and the availability of sensing infrastructure put in place to monitor various quantities soars, there are clear benefits in a model where infrastructure can be shared amongst multiple applications. This model however introduces many challenges, mainly related to the management of the communication of the same application running on different network nodes, and the isolation of applications within the network.
At the same time, security concerns related to terrorism, crime, and lower-level anti-social behaviour and fraud have placed pressure on government agencies to be seen to be doing something to respond. Extensive surveillance is the easy option, as already seen in the UK with the installation of millions of CCTV cameras and a political fondness for the "database state"[ABD+09]. The emergence of low cost pervasive sensing will present another tempting target for surveillance. While there may be legitimate reasons for situational awareness from time to time, placing all citizens "under the microscope" 24/7 has a well-known corrosive effect on society[Fun04].
Thus, the combination of dynamic requirements for privacy, and occasional surveillance results in new security challenges. In this paper, we describe the Fresnel project's technology[ELMC10] that addresses these challenges. We tackle these by design methodologies, and integrate solutions with each sensor application, and provide a substrate that enforces appropriate levels of privacy and separation of roles and rights to data, within a virtualised sensor networked OS.

1 Introduction

There is now an overwhelming wealth of data sources in the world reporting on what they sense. Many of these are simply monitoring heating, ventilation and air conditioning (HVAC), for the purpose of accounting for energy. Some also contain actuators for decentralised control[1]. Many others, though, explicitly afford a view onto human activities[2]. In the extreme, cameras and microphones transmit to

[1] Much has been written elsewhere about the risks of such systems, and so we will not cover that further here.
[2] Even the simple HVAC data can be used to infer human behaviour — someone's presence in a building is usually associated with higher energy use.

remote recording facilities, which can then be used to construct a complete timeline of peoples' lives.

Increasingly, these systems are being integrated together, to reduce networking costs and simplify systems management. Just as the Internet knits together many sources of documents, so the Internet of things weaves together many sensory (and control) systems. It is tempting to think of this as a global autonomic nervous system, by analogy with the sensory and nervous system of a human. This analogy leads unerringly to the obvious step of centralising all the sensed data and processing it in a single "brain".

Security concerns from government agencies has led to mission creep, creating a "database state"[ABD+09] and a "surveillance society"[Gil07]. In some cultures, there has been grassroots resistance to this creep, but the UK's Information Commissioner has warned that "we are in fact waking up to a surveillance society that is already all around us"[Ben06]. Using the Fresnel project as an exemplar, this article is a reminder that systems with appropriate checks and balances can be built by design[Cav], at a lower cost than the naive ones with the associated risks described, such as potential total privacy loss, and a shift to the unpleasant mode of society consisting of everyday paranoia amongst everyday citizens.

Back in the 18th century, the philosopher Jeremy Bentham designed the Panopticon. This was a building structure intended for prisons, which afforded a view of all of the inmates' cells from a small number of vantage points. This would increase security, at the same time as reducing costs[Ben95]. Note that the reduction in privacy (and a number of other rights) is something that can be discussed legitimately as part of the justice system. A Panopticon model of everyday society is a rather radical step to take outside of prison walls.

Furthermore, the centralisation of information into a single "sensory cloud" allows as many vantage points as there are people. We might think of this as a Pan-Panopticon, where everyone can look at everyone else, all the time. In the Fresnel project[LEMC12], we have researched user attitudes into such systems in a work environment. Participants do express some concerns about their privacy, where a significant fraction questioned whether such systems might be used to measure workplace performance, for example[ELP+12]. This has led us to consider the design of sensor systems that permits technological integration, while still controlling the flow of information, even restricting it at source if necessary, and by design. We describe this system in the next section.

2 Fresnel

Fresnel is an EPSRC-funded UK project between Oxford and Cambridge universities to build new tools and techniques for federating sensor networks[3]. As with the original design for federating networks in the Internet, policy and mechanism for controlling the flow of information between different domains is essential. To this end, there are two key techniques employed in our approach:

Virtualisation Firstly, the sensor network is virtualised at the node and network layers[LEMC12]. This enforces isolation between applications (just as in virtualised services in the cloud), so that the designer, implementer and operator of a

[3] EP/G070687/1

particular *slice* of sensor network cannot observe traffic or behaviour in another *slice*.

Resolution Secondly, we employ techniques to reduce the resolution or accuracy of data recorded, *at source*, and by design, for example, with location reporting, deliberately fuzzing the data[QLM+11], to retain privacy.

These techniques reduce the risk of misbehaviour by the system operators and owners. However, the lower-resolution sensor data is still reported and can be recorded. Thus it is still possible for someone to process several different sources of data and integrate the results over time and space, increasing the accuracy with which they can observe people and thus reduce their privacy.

Socio-technical and legal mechanisms are required to mitigate these remaining risks, which we argue will become incumbent on sensor network operators under the EU's Data Protection Directive[PC95]:

1. Under Article 10 of the Directive, individuals need to notified that their personal data is being processed, and by whom. This is normally the case with surveillance cameras used for security (e.g. for gathering evidence of shoplifting), where signs have to be made visible to inform people of this fact. This should be extended into the sensor world in general. One could imagine a simple application on one's smart phone alerting the user to the presence and purpose of sensors and the destination of any sensed data, and proposed usage. Thus *including in* the subject of sensing allows them to make a decision (to prevent use of data, or opt out of the situation). In some sensitive situations, opt-in consent might be required.
2. Article 17 of the Directive further requires that "appropriate technical and organisational measures" are taken "to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network". Sense-data should be encrypted, before transmission and during storage. Thereafter, access to the data should be restricted to approved users and usage, and audited. Access should also employ techniques such as homomorphic operations for privacy preserving queries, and differential privacy tools, to reduce the statistical inferences that can be made from such data.
3. Article 6 of the Directive requires that personal data are "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed". Identifiable sense-data storage should have a strictly enforced expiry date (which can be checked by the user and third parties). Here, legal and economic penalties must be used to incentivise the sense-data storage sites to behave properly (at least until some researcher devises a method for *provable deletion*).

We believe that this combination of approaches is both viable and desirable. Indeed, large scale deployment of such techniques has been seen in the commercial sector — for example, the default in the London Congestion Charge system (in its second generation implementation) is to process video of car registration plate data *within roadside units* and having recognized a number associated with a payment, simply not to record anything or send the number to a central processing centre. Only in the case where there is no payment record (which are broadcast to the units) does the image need to be sent (including a human-in-the-loop for verification) to the database to issue a notice to the vehicle owner. If the owner pays within the time allowed, the record can then be immediately (and permanently) deleted. One can extend such design ideas to many other systems.

3 Conclusions

In this paper, we have described the Fresnel project, which has been researching techniques for federation of sensor networks. Our aim is to reduce deployment and operational costs for sensor systems, whilst at the same time employing tools for reducing the risks to privacy inherent in the naive approaches to date. These include mechanisms for the distributed enforcement of security and privacy policies across a federated sensor network.

We would also note that many of the data reduction techniques (e.g. reducing fidelity of video data) have the added benefit of massively reducing the amount of data moved across the sensor network. Since these devices are frequently battery-powered and hence limited in processing and transmission resources, this has the side-effect of prolonging their lifetime and reducing operational costs (e.g. of replacing batteries) and so aligns incentives between retaining privacy and operational economics.

References

[ABD+09] Ross J. Anderson, Ian Brown, Terri Dowty, Philip Inglesant, William Heath, and M. Angela Sasse. *Database State*. Joseph Rowntree Reform Trust, York, 2009.

[Ben95] Jeremy Bentham. *The Panopticon Writings*. Verso, London, 1995.

[Ben06] Jason Bennetto. Big brother britain 2006: 'we are waking up to a surveillance society all around us', November 2 2006.

[Cav] Ann Cavoukian. *Privacy by Design*. `http://www.ipc.on.ca/images/Resources/privacybydesign.pdf`.

[ELMC10] Christos Efstratiou, Ilias Leontiadis, Cecilia Mascolo, and Jon Crowcroft. A shared sensor network infrastructure. In *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*, SenSys '10, pages 367–368, New York, NY, USA, 2010. ACM.

[ELP+12] Christos Efstratiou, Ilias Leontiadis, Marco Picone, Kiran Rachuri, Cecilia Mascolo, and Jon Crowcroft. Sense and sensibility in a pervasive world. In *Pervasive 2012*, 2012.

[Fun04] Anna Funder. *Stasiland: Stories from Behind the Berlin Wall*. Granta Books, 2004.

[Gil07] Nigel Gilbert, editor. *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*. The Royal Academy of Engineering, London, March 2007.

[LEMC12] Ilias Leontiadis, Christos Efstratiou, Cecilia Mascolo, and Jon Crowcroft. Senshare: Transforming sensor networks into multi-application sensing infrastructures. In *EWSN*, pages 65–81, 2012.

[PC95] European Parliament and Council. Directive 95/46/ec of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, November 23 1995.

[QLM+11] Daniele Quercia, Ilias Leontiadis, Liam McNamara, Cecilia Mascolo, and Jon Crowcroft. Spotme if you can: Randomized responses for location obfuscation on mobile phones. In *ICDCS*, pages 363–372, 2011.