How to Create Oversight in Intelligence Surveillance

JOUNI VIITANNEN, PASI PATAMA, JYRI RAJAMÄKI, JUHA KNUUTTILA, HARRI RUOSLAHTI, TUOMO TUOHIMAA & ILKKA TIKANMÄKI
Laurea SID Leppävaara
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo
FINLAND
jouni.viitanen@laurea.fi http://www.laurea.fi

Abstract: - To prevent and investigate crimes, Law Enforcement Agencies (LEAs) are conducting various operations which are affecting privacy of citizens. These activities include video surveillance, audio surveillance and technical tracking. Currently, LEAs has power to conduct these operations based on legislation. While law enforcement is applying for more rights based on jurisdiction, public concerns are rising up and open discussions growing. Does a LEA really need broader ways to do surveillance, and are they enforcing the rights they already have in ways which are described in legislation? These concerns are often brought in discussion against rising power of surveillance state. Is it possible to be found a balance between a LEA's operational security needs and individuals' freedom? This paper outlines a scenario how common ground can be found with a constructive approach facilitated by advanced technology. First part of this study shows the need for transparency, because without it there might be no new legislation that LEAs might get. We have evidence that Citizens are willing to give more power to authorities if usage of these intrusive means is more transparent and better monitored by public. Second part of the study shows examples of today's technological possibilities to create transparent and plausible monitoring for surveillance activities. How would it be possible to credibly show peoples that powers are used according to the law? In this part, we describe a system evolving ubiquitous but transparent surveillance, and what kind of difficulties there might be.

Key-Words: - Law enforcement, Legal audit, Oversight, Privacy, Public safety, Surveillance, Trust

1 Introduction

This paper tries to look forward, how is possible to create a law enforcement surveillance operation that can be approved by the citizens. This subject is a spin-off of the SATERISK project, which is e.g. looking to risks in GNSS-tracking [1].

A Finnish Ex- Minister and Member of Parliament wrote in his blog [2]: "I have always been somewhat suspicious about the drug police's demands to get more powerful eavesdropping systems. There is no use for these systems. If police has the right to listen in telephone conversations, no one will tell secrets on the telephone, and so on. And there will always be someone who will misuse those rights."

'Mike' McConnell, a former director of United States National Intelligence, has said [3]: "…we all want security, but won't give up our privacy … so we have to rethink intelligence, reshape it, and were not there yet … any bureaucracy can do evil … there must be oversight…"

The European Union anti-terrorism legislation required telecommunications operators to retain phone data and Internet logs for a minimum of six months in the case they are needed for criminal investigations [4]. German Law had then ordered that all data – except content – from phone calls and e-mail exchanges be retained for six months for possible use by LEAs who could probe who contacted whom, from where and for how long.

The Federal Constitutional Court of Germany ruled that this law violated Germans' constitutional right to private correspondence and failed to balance privacy rights against the need to provide security. It did not, however, rule out data retention in principle. "The disputed instructions neither provided a sufficient level of data security, nor sufficiently limited the possible uses of the data," the court said, adding that "such retention represents an especially grave intrusion." The court said, that because citizens did not notice the data was being retained it caused "a vague and threatening sense of being watched." [5]

In abovementioned cases, the bottom line is the trust. Terrorist attacks and other serious crimes are happening around the globe, Germany is not an exception. Despite of it, circa 35,000 Germans have appealed to overturn the law. People seem to be willing to take a chance with terrorists and criminals because they fear that a LEA is abusing its powers and

intruding their privacy. These cases are not even as intrusive as technical tracking or eavesdropping. If police is utilizing the specific phone call or e-mail exchange data, the operator's system and log files will have marks that the copy of the data has been delivered to the LEA.

In cases when a LEA is using its own room audio recording or technical tracking systems, the trust building between citizens and LEAs is even more difficult. In cases of call detail records data utilizing, there will always be a log file mark in the operator's system and that leaves a trace. However, LEAs are still using some stand-alone systems, where no log marks are created.

In Finland, the oversight of police's coercive usages is based on a file system SALPA that the National Bureau of Investigation runs [6]. The SALPA system guides, how to make applications and notifications in the correct manner. But, could this system alone be a sufficient legality control system, if the information that police officers write down are not based on actual log files?

These non-transparent systems might be handicaps to LEAs. The LEA may act so that everything is done according to the law. However, they cannot prove it because methods cannot be audited by an outsider. The LEA can only claim that they are doing the right thing. These claims are challenged periodically but always afterwards when the Ministry of Interior is conducting legality inspection to see how operations are conducted and documented. This is not a very efficient and transparent way of operating. With the lack of trust, there is a lack of new legislation that allows usages of new crime fighting tools. With this situation, everyone is losing something; security. We believe that there is a way to find balance between security and individual freedom and to find common ground between good will approach and taking advantage of advanced technology, resulting in a powerful law enforcement tool open to third-party review.

Finnish futurologist Mannermaa says that the society is presented as "soft surveillance, knowledge and non-forgetting history data". The important difference between 'Some Brother Society' and Orwell's 'Big Brother' is that in a 'Some Brother Society' surveillance is commonly agreed upon and transparency. An important point is that when information society's first stage deepens to 'ubiquitous network society', single-sided enforcement and surveillance is straining people. Within ubiquitous network society, it is possible to create multi directional surveillance and develop transparent authority power. [7]

2 Material and Methods

This study is going to explore already available technical possibilities to build surveillance operations according to the 'some brother' vision. Scenario time lines are usually 10-20 years and since Mannermaa has stated his vision already two years ago and it is obvious that new reformation is going to take time. If we want to see results in the original 10 year timetable, we should see signs of implementation acceptance already now. Though commercial markets are not yet visible, we should see signs of acceptance in society and technology should provide possibilities to support this ubiquitous realization already.

This study is divided in two parts. The first part of the study looked at the citizens' willingness to give more power to authorities if the usage of these intrusive means is more transparent and better monitored. This part is conducted by questionnaire. The second part, concerning design research, looks at possibilities to create transparent and plausible monitoring of surveillance activities on both levels of technology and processes used by authorities in this field.

How would it be possible to credibly show people that power is used according the rights and in ways benefiting people? In this part we describe in theory what systems evolving in this direction would be like and look at what is possible to achieve and what kind of difficulties there might be. As part of this surveillance authoring process, we could also see methods of open acceptance processes in technology which are used to conduct these intrusive operations. By opening this process of technological development to publicly accepted review processes we could reach levels of assurance in a wider scope. In surveillance security is important and security through obscurity is not enough.

3 What is wrong with Surveillance Society?

In big cities we already live already in a ubiquitous surveillance society. In all the rich countries the cities suffused with surveillance encounters, not merely from dawn to dusk but 24/7. Massive social and technological advances have occurred in the last few decades and will continue in the years to come. Some think surveillance is as a malign plot hatched by evil powers and others think that it is the only way cut crime. Surveillance is always two-sided. Within both these sides, benefits and downside must be acknowledged. One guard looking a street view and people with two cameras is normally not apple to get

much information. But a network with cellular phone triangulation, on line search queries, loyalty cards etcetera, you really can get in persons private life.

4 The Ways in Which We Can Be Watched

There are safeguards against the abuse of surveillance by LEA. The LEA use of surveillance is one of the most regulated of any group in society. But still many people are particularly concerned about the unseen, and what as they think is uncontrolled or excessive surveillance. Here as an example a list from a BBC story how we can be watched [8]:

* 4.2m CCTV cameras
* 300 CCTV appearances a day
* Reg plate recognition cameras
* Shop RFID tags
* Mobile phone triangulation
* Store loyalty cards
* Credit card transactions
* London Oyster cards
* Satellites
* Electoral roll
* NHS patient records
* Personal video recorders
* Phone-tapping
* Hidden cameras/bugs
* Worker call monitoring
* Worker clocking-in
* Mobile phone cameras
* Internet cookies
* Keystroke programmes

Luckily, only LEAs can legally obtain information from all these sources. Unfortunately, large-scale technological infrastructures are prone to large-scale problems, and we can read about data leakage almost daily from the newspapers. Fortunately, it is really difficult for a cracker to get all the information about one person.

There are allegations about LEAs abusing surveillance. Most LEA officers are answering, that they are not abusing surveillance. Unfortunately, they cannot prove the case otherwise, because the case and material are confidential and publicly not available to use as argument. LEAs are claiming that any of the police surveillance that is unseen is in fact controlled and has to be proportionate otherwise it would never get authorized. To faultlessly control something like this means that you must have faultless control of the surveillance equipment all the time. How is this possible and how you can prove it to the public?

5 Weak Signals

So we went to look for weak signals. We have already two: 1) the Member of Parliament writings, that in any case LEAs' are prone to abuse these systems, and 2) the judgement of the German constitutional court. Then there is a growing number of con intelligence organizations like Privacy International, Surveillance-Studies Network and Civil Liberties Union. Does this mean that people are plainly just against surveillance? Are common people willing to exchange privacy to security and are they more willing to do so if the systems are more transparent. To find out this we made a poll of 80 people answered. There we can see the need for transparency because without it there might not be new legislation that meets LEAs' needs. The poll was to pupils at the Laurea University of Applied Sciences. There were two basic groups, business students and security students. Tough the number of answers was only 80, but it was enough for the purpose of finding out if weak signals existed, not yet in this phase to get to the bottom of it.

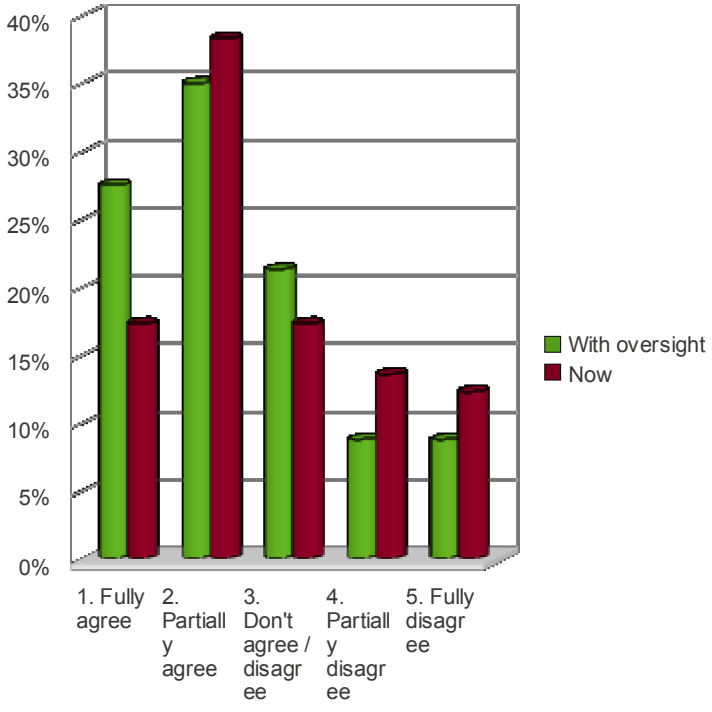

Fig. 1. Poll on willingness of conceding more powers for LEA

In Fig. 1., the red columns presents those who want to give more jurisdiction based rights to LEA in current circumstances; there only 17.3% fully agreed. The green columns presents those who are willing to give more jurisdiction based rights when given assurance that LEA is not abusing its powers; there 27.5% fully agreed. This was our first small (n=80)

ISBN: 978-960-474-286-8

poll just to find, if the phenomenon existed. We did find that there is a remarkable shift. From these columns, a shift can be seen to pro more powers to LEA, if people can be sure that LEA is not abusing them.

The fact which makes it even more noteworthy is that in the 2007 Police barometer (n=989), 48% of Finns trusted the police fully and 46% for most part [9]. So only 6% had not trust in police. In Finland, police is by far the biggest law enforcement agency. So, even when there is wide and good trust base, there is still a need for more transparency.

What we can see here is that citizens are more willing to give more jurisdiction based rights, if they have more trust to the system. This is the fact why we think that a growing number might say yes to more jurisdiction based rights to LEA, if they are more certain that LEA is not abusing its powers. The trend is there, so in that sense of Mannermaa's vision of the future development might be possible.

6 Technical Solution

For this paper, we have made a Proof of Concept (PoC) system which is described in Fig. 2.

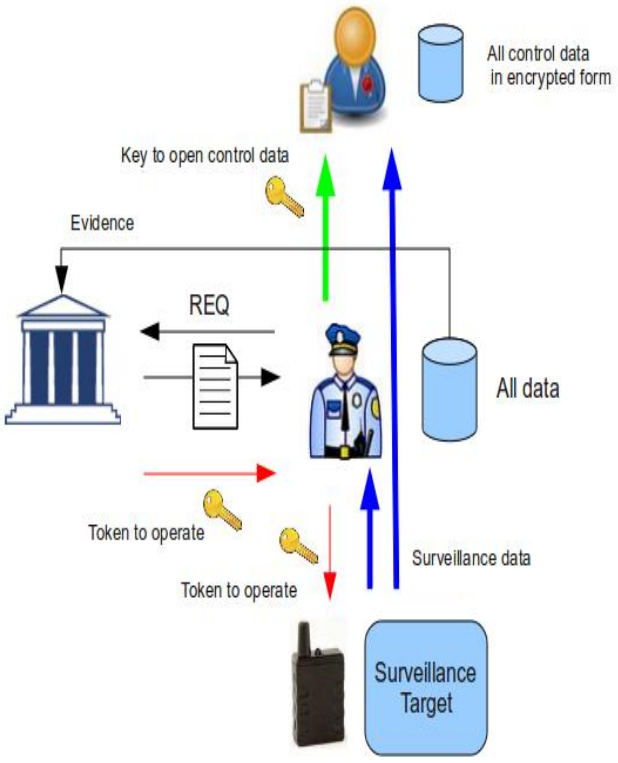

Fig. 2. System for transparent surveillance

The 'surveillance data' is consumed by Police (blue line in Fig.2). Surveillance data is also delivered simultaneously to the oversight officer (blue line). When the oversight officer (or party) wants to audit conducted operations, he calls Police to visit him and bring accessing key for data (green line + key), REQ(uest) and Court order (black line between police and court). When Court issues mathematical token (red line + key), Surveillance equipment accepts court issued token and sets parameters to operation as ordered (from court order) (red line + key). From surveillance target, equipment collects data (blue area) - "substance". So, all data is stored by Police and the Oversight officer, but permitting to audit data contents can only happen with operation decryption key from police and no leakage is possible without Police presented decryption key.

Nowadays, it is possible to use publicly accepted and reviewed authentication and cryptography functions to authorize and control deeply privacy invading equipments and data they produce. And to gain publicly accepted operation schemes in these surveillance operations. However, this requires commonly agreed ground, where device manufacturers and surveillance power projectors (police, intelligence) are authorized to obtain technology to fulfil this principle.

The technology and procedure to be used in the given scenario consist from several parts. Notably, the biggest difference compared to current situation is that the PoC system is centralized and parts are only working together and no ad-hoc usage is possible. The Process parts are Court (instance of permissions), Police (instance of cases and operations), Legal audit (monitoring, auditing and inspections of coercive means) and Target (surveillance operation target).

For this paper, we implemented PoC which brings transparency and trust to shady surveillance operations without disclosing any confidential parts of operations to any unauthorized party.

For this approach, we identified most intrusive parts used in these operations and data they produce. These are surveillance equipment and data which they produce. As long as these pieces of equipment are capable to operate without authenticated permission token, there is no means to control their usage. No process or instance is able to present publicly accepted proof of correct use of these pieces of equipment as long as there are no publicly proven technical control methods involved in the chain.

The same applies to the data they produce. There are some recognized evidence authentication needs and schemes in both legalization and technology, but it is not capable to fully expose when, where and by

whom data is produced and is surveillance data obtained under permission granted.

When coercive means are used, acting authority should be challenged with these questions:

- Is equipment capable to operate without technical authentication token?
- If equipment is used, who gains awareness of operation?
- Is there a possibility to 'try' to do operation with surveillance equipment and if it succeeds, do the permission paperwork later?
- If there is produced data, can we identify amount of produced data?
- If equipment is run over period of time, could we assure that control of technology has been under acting party control all that time?

7 Conducting Operations with PoC System

Opposite to traditional surveillance operations, where equipment is taken to the case, used and material is extracted - our implementation includes chain of trust between the process parties. Making it possible to create a transparent and yet secure surveillance operation base. Transparency is based on technology which supports operations legal processes firmly, making it possible only to obtain surveillance material with technology authenticated to operation. For oversight, all the data from the source is sent in encrypted form to a trusted third party (ombudsman etc.), a trustee of the public. This trusted third party can not see the actual data until the representative of the LEA is present with the decryption key. This is the way how secrets stay as a secret, and "black" operations are impossible.

8 Conclusions

The public economy will still be weak for some years. This means that many parties suggest saving money in law enforcement by using less manpower and more surveillance technology. In some points that leads for the need of new legislation for LEA. We believe that people are willing to give new powers if they can be sure, that LEA is not abusing its powers. What LEA officers need to understand is that there might not be new legislation and further no use of new technology, if the systems are not linear and transparent.

As a part of the surveillance authoring process, we could also see methods of open acceptance process in technology, which are used to conduct these intrusive operations. By opening this process of technology development to publicly accepted review process we could reach level of assurance in wider scope. In surveillance operations, security is important and security through obscurity is not enough.

Technically, it is possible to generate real oversight for some LEA systems that already are in use. In this case, the computer systems and surveillance equipment in law enforcement will only be a little more complicated and only marginally more expensive. The foundation for a trip towards the 'some brother society' is there already.

References:

[1] http://www.saterisk.fi
[2] O. Soinivaara, web block. *Narcotic Police under suspicion* in Finnish, 10.12.2007.
[3] T. Shorrock, *Spies for hire*, Tantor Media, 2008, p. 55.
[4] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
[5] German constitutional court, Germany Federal Constitutional Court overturns data retention law, 2 March 2008
[6] Finnish National Institute for Legal policy, Telecommunications surveillance and legal protection in Finland, 2009.
[7] M. Mannermaa, Jokuveli – *Elämä ja vaikuttaminen ubiikkiyhteiskunnassa (Some brother society)*, WSOYpro, 2008 [in Finnish]
[8] BBC news story, *how we can be watched*, BBC London, 2006/11/02
[9] Finnish ministry of interior, *Police barometer 2008*