European
Commission

This project has received funding from the European Union's Seventh Framework Programme for research; technological development and demonstration under grant agreement n: 607480

LASIE

LARGE SCALE INFORMATION
EXPLOITATION OF FORENSIC DATA

1st LASIE Roundtable session minutes
"Ethics vs. efficiency in content extraction for digital evidence"

LASIE Project

FP7 - SEC-2013.1.6-1 - Framework and tools for (semi-) automated exploitation of massive amounts of digital data for forensic purposes – Integration Project

Grant Agreement n°: 607480

Start date of project: 1 May 2014

Duration: 42 months

Document. ref.:

1st LASIE Workshop
London, UK, 15 July 2015

version 6 final

Roundtable Session

Ethics vs. efficiency in content extraction for digital evidence

A public report
compiled by César Pantoja Sánchez (QMUL) and Dr Tomas Piatrik (QMUL)
reviewed by Dariusz Kloza (PRIO), Stine Bergersen (PRIO) and Claudio Massari (INNEN)[1]

1 Introduction

The LASIE project,[2] or 'LArge Scale Information Exploitation of Forensic Data' (2014-2017), is a research project co-funded by the European Union (EU) under the 7th Framework Programme for Research and Development (FP7), which aims to '*design and implement an open and expandable framework that will significantly increase the efficiency of current investigation practices, by providing an automated initial analysis of the vast amounts of heterogeneous forensic data that analysts have to cope with*'. Nominally, it is – as the partners call it amongst themselves – a 'gadget'-project, i.e. designing, developing and validating a tool constituting *de facto* a surveillance technology, and the vast majority of partners' effort focuses thereon.

Acknowledging the fact that the development, design and implementation of such a 'gadget' can produce secondary societal impacts, the LASIE consortium comprises a partner responsible solely for legal and ethical compliance, i.e. the Peace Research Institute Oslo (PRIO). In addition, a significant part of the consortium's activities is devoted to the ethical and societal responsiveness of both its work and its final product. Furthermore, what is more important, the consortium wishes to be involved in a discussion on the reconciliation of the needs and efforts for the efficient post-crime investigation, on the one hand, and on ethical responsiveness of these needs and efforts, on the other. Ultimately, the LASIE consortium wishes to take the results of such a debate into account while their 'gadget' is being is developed and at the same time pave the way for further research projects.

Amongst plenty of forums in Europe for debating the impact of technology on the society, not many of them originate from technology developers. With a view to improve that, and following a successful debate of that type, held by the sister project ADVISE, or 'Advanced Video Surveillance archives search Engine for security applications',[3] on 25 November 2014 in Pont-Saint-Martin, Val d'Aosta, Italy,[4] as well as a roundtable at the 8th Computers, Privacy and Data Protection (CPDP) on 21 January 2015 in Brussels, Belgium,[5] the LASIE consortium has decided to organise their sequel during the 1st LASIE public workshop, itself meant to communicate the project's developments thus far to the end-users and to seek their feedback.

Consistent with the foregoing, the roundtable session "*Ethics vs. efficiency in content extraction for digital evidence*" was held on 15 July 2015 in London, UK, at the premises of Queen Mary, University of London (QMUL), and consisted of two contrasting panels. The first panel was composed by end-

[1] Contact persons: Claudio Massari (c.massari@innovationengineering.eu) and Dariusz Kloza (darklo@prio.org). We thank Dr Lucas Melgaco for his useful input.
[2] Cf. http://www.lasie-project.eu.
[3] Cf. http://www.advise-project.eu.
[4] Cf. http://www.ies.be/node/2649.
[5] Cf. 'Boiling the Frog: Roundtable on (Privacy) Impact Assessments as a Response to (Smart) Surveillance', http://www.cpdpconferences.org/Resources/CPDP2015_PROGRAMME.pdf.

users, i.e. representatives from law enforcement authorities (LEA), and the aim here was to discuss their respective needs and requirements relating to privacy, personal data protection and ethics. The second panel was composed by experts in ethics, privacy, personal data protection and forensics, as well as by policy makers and academics (researchers) working on European projects related to security and surveillance. This second panel was meant to be a response to the end users' statements made in first panel.

A moderator, who had in advance notified the speakers of the questions for discussion, chaired each panel and – with a view to have a vivid discussion – allowed each speaker only two minutes sharp to answer each question. The time allotted was strictly respected. Having concluded each panel, there was a short discussion with the audience.

To ensure the openness and frankness of the debate, the meeting was held under the Chatham House Rule, i.e. "*When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed*."[6] Therefore, although the names of participants, upon their agreement, were made public in advance, the statements they made in this roundtable were not linked to them.

The present report offers a succinct account of the views expressed during the roundtable. It is meant to constitute a 'raw' material for further debates on the impact of technology on the society. On top of that, the editors of this report have selected some concluding key observations.

The views expressed in the following are solely those of the speakers and/or editors, and can in no way be taken to reflect the views of the LASIE consortium as a whole as well as its individual partners nor the European Commission.

2 First panel: Perspective of Law Enforcement Agencies

Chair: Dariusz Kloza (PRIO, Norway)

Participants:

- Mr Jonathan Betts (Home Office, UK)
- Mr Federico Urìa (Police of Madrid, Spain)
- Mrs Luisa Proença (Policia Judiciaria de Portugal)
- Mr Andrew Ramsay (Leicester Police, UK)
- Mr Richard Beckely (Metropolitan Police – Scotland Yard, UK)

1. What are the challenges faced by law enforcement agencies in which electronic surveillance systems can play a role?

A representative from a LEA stated that we need CCTV because we need to see a story, and that 'the story' is important for prosecution. What interests the police officers in the first place is where the footage is located and where evidence is stored. In court, they sometimes say they do not care about privacy protection mechanisms like watermarks and filters, they just want to know where the footage has been captured and stored, so they get quick access to it and start with investigation. Another representative said that we have too much information and databases, but the challenge is how to put all this information together, and correlate everything to help investigators do the job. Accordingly, the biggest challenge is how the amount of information that is available to improve criminal investigation can be used.

Then, another LEA representative said that one of the challenges is the use of technology. This stems from the fact that technology is constantly being updated, and has to be aligned with the relevant regulations from the EU and its Member States. We not only need to deal with many types of cameras, but also open source systems. This means that law enforcement are constantly challenged by and faced with, a diverse range of evolving

[6] Cf. https://www.chathamhouse.org/about/chatham-house-rule.

technologies. Another participant said '*I'm doing everything to do with recognising faces. The biggest challenges are that most of the cameras are taken as "Big Brother". What we have to do is to make sure these technologies are used to help to solve crime and not serve watching people*'.

The next LEA representative went on to say that the challenge is to use technology to help solve the crime and improve the technology so that it does serve society and help investigators catch criminals.

2. In what areas do such surveillance measures come up against out-dated legal and ethical norms?

The first LEA representative said that the keyword is the management of data. There is so much data that it turns dangerous. The potential (security) breach is huge. It is difficult to keep up with such huge amounts of data and it is difficult to keep up with training people. This is what LASIE is doing well and it is important for the project to cover.

Another panellist added that the issue should be to find the right balance between finding evidence and protecting privacy. The challenges are so big that it is difficult to strike this balance. It is becoming problematic to be able to correlate systems, but it is important to do the best to get this balance. Then the next representative from law enforcement stated that in their country they have very restrictive data protection laws. There must be a balance between criminal responsibility, and law that protects criminals. Politicians make laws and it is challenging for the police to follow the law and protect people at the same time.

The next participant asserted that when going for holidays he knows police will take care of him and they are not going to spy on him. It is just a misinterpretation if people believe that the police are spying on them. Face recognition works and the police are doing great work to find criminals. It is only a misinterpretation that the police is acting like a "Big Brother".

Then, another participant shared that they tend to look differently on things like data protection in their country, as they follow a more pragmatic approach to data protection, and allow doing things that "needs to be done". Another point is that data know no boundaries. The LEA representative wonders why is it that they can get data from one country easily, but not from other, and stresses that it needs to be easy to share data, for the purpose of serving the society.

3. Are there any side effects for society stemming from enhanced surveillance measures?

The first panellist voiced that crimes *have* in fact been solved by the use of CCTV, and that in their country, people are complacent about CCTV for many reasons, one of them being that the country does not have a political history of dictatorship. He elaborated that finding the right balance between security and privacy, and educating the population, are keys to success. Another LEA representative then went on to say that in our digital society, we use technology in a lot of aspects in our life without hesitation, but when technology is used in the surveillance domain, people will see it as something dangerous. Due to recent terrorist attacks, people are more willing to be surveilled, but compromises must be made, between surveillance and privacy.

Another speaker then recognised that citizens are reluctant to surveillance because of privacy concerns, but that compromises must be made, e.g. to reduce our privacy to be more secure, and that this "trade-off" is what makes such systems unpopular. The next speaker mentioned a particular case of a murder in the 1980s in their country, where they could have caught the perpetrator easier had they have access to CCTV, but everyone still blames the police because they did not catch the murderer sooner regardless. A reason for this could be that many people generally have a certain level of distrusts towards new technology, as could be seen when DNA tests were introduced.

The fifth participant stated that surveillance measures have negative consequences, but for the criminals, terrorists, etc. This participant confirmed that the lack of dictatorships in their country affects how people perceive CCTV, as the society might have vested more trust towards their governments. But when surveillance is misused (like for political prosecution), people will start to distrust. And for that, safeguards must be in place to prevent this from happening.

4. What is the difference between policing and national security? Does it necessitate different surveillance systems?

The first speaker answered that both work for the same end, but policing works within the community, and trust in the police depends on checks and balances. National security operates wider and broader, and trust is not guaranteed.

The next person said that policing works usually under respect of the law and must comply with the law and all its constraints. In national security, there are not so many constraints in the law, and more things are possible. The third speaker then answered saying that the differences are clear. For example, in the US the motto of some police departments is "to Protect and Serve". This shows that policing is a more "human" activity.

The response of the fourth participant was that people in surveillance positions must be policed and punished if they misuse the tools and information they have access to. In national security, information is usually not shared and there is a lot of mistrust intra- and inter-department. The answer of the fifth speaker was that they fight organised crime and terrorism respectively. They are different, but also they have many similarities, and there are a lot of overlapping and synergies. To ensure the correct use of the tools, a good set of values, which are scalable regardless of the size of the crime, are needed.

5. Questions from the audience

The first question from the audience was a statement that regulators do not usually understand technology and policing. This petitioner thinks this must change and the panel agreed. Following the statement of difficulties in mutual understanding, the moderator then gave an example of some confusion in an interdisciplinary research group over the use of the word "ontology", pointing to the fact that it has a technological meaning as well as a philosophical one.

The next question was regarding the (negative) reaction of the press and public over the use of face recognition software in a recent mass event in the UK. One of the panellists answered that it was only used to catch criminals and drug dealers, and that the negative reaction was caused by a misunderstanding by the public. It was actually merely a trial of an already existing technology. This speaker underlines that the press are just looking for a sensationalist story to sell.

The next remark from the audience stated that people can be said to be hypocritical about the use of their personal data, as they hand their information willingly to companies like Google or Facebook, but sharing the same information with the police is considered as a bad practice. One of the panellists thinks that there are pockets in Europe where you have countries like France and Germany that are very sensitive to privacy but, for example, the UK is not. Another panellist intervened, noting that police actually do go to social networks as part of their investigations and that the practise has proven useful. A member of the audience then stated that this is an oversimplification, because our profiles online are carefully crafted profiles or identities. The same panellists then replied that there is no (or should not be) a difference between patrolling social networks and real life. Another speaker then mentioned that people do not really know how companies like Facebook or Google work, and they are not willingly giving their information. A LEA representative further said that people do not reflect upon the consequences when posting information online. The moderator remarks that people must be educated on this.

The next question was about the critical points when dealing with surveillance systems. One of the LEA representatives does not like the word "balance". Another speaker thinks we should be more mindful of the long-time societal (?) effects, as for example there might be governments with different intentions governing in the future. A third speaker thinks citizens should let police do their job and give consent to them the same way they give to companies like Google or Facebook. Another one added that the police should get punished when misusing the means and they should prevent this from happening. The fifth speaker thinks again that there should be a balance between security and privacy, and questions the authority the police have in looking at people on the street, and what is the role of police in our society. The first panellist again intervened by saying that it is necessary that safeguards are in place for corrupt police as there are currently not many and that this must change. Another speaker contributed saying that preventing and protecting are two different tasks.

3 Second panel: Perspective of Social Scientists

Chair: Dariusz Kloza (PRIO, Norway)

Participants:

- Prof Silvia Ciotti (Eurocrime, Italy)
- Prof Zeno Geradts (ENFSI Forensic IT Working Group, the Netherlands)
- Mr Alfonso Alfonsi (P-React project, Italy)
- Mr Stephen Crabbe (3D-Forensics project, Germany)
- Dr Ben Hayes (PRIO, Statewatch & Transnational Institute, Norway/UK)
- Prof Kostantinos Rantos (Eastern Macedonia & Thrace Institute of Technology, Greece)

1. **What technologies, fuelled by information, would never be accepted by the society? In other words, where lies the thin red line between socially acceptable and unacceptable surveillance?**

The first speaker in this panel answered to this question that those surveillance systems that are too invasive to humans rights would be unacceptable. The next speaker thinks that this line lies at being physically monitored (like with wristbands), but points to the fact that people are already starting using so-called wearables. This speaker thinks that ethics is not a static thing, and that what is ethically acceptable varies by country and time. Consequentially, if people accept something, it is acceptable, but only for that particular context and the particular point in time.

Another speaker argues that a line cannot be drawn on a single technology, as acceptability is highly subjective. This speaker adds that some people do not want to be "active", but they want privacy. They do not want to take any action themselves to protect their personal sphere, they expect the providers of technologies to take care of that. Furthermore, surveillance should allow people to choose. The fourth panellist thinks that anything that disturbs our privacy is crossing the line, but this is ever changing and it is also relative. Nowadays people tend to share everything, and in a few years, wearables and the Internet of Things (IoT) devices will be even more invasive. If we give our consent, it is legal, and if it is not hidden, it will be – from a formal point of view – fine. The moderator then gave an example where urinals were being used to test for drugs. In such a scenario, people are under permanent control and this crosses the line of social acceptability.

The fifth speaker mentions that the definition of surveillance is "tracking and observation", and this should be implemented while respecting e.g. the minorities in society. The sixth speaker argued that even if we *do* draw a red line, it would change soon, but the values of the people will not. This panellist mentioned a scandal recently in the UK because the Government Communications Headquarters (GCHQ) was spying on people's webcams.

2. **The surveillance industry continues to develop more and more invasive technologies, but actually not many of them fulfil hopes vested therein, not many are widely accepted and/or used in practice. Can you analyse an example from your own experience?**

The first panellist mentioned an example were a system was devised to track which camera had taken a particular picture for forensic evidence. It took a long time to implement, and to process, and police had a lot of problems. It did not go as originally intended. The second speaker thinks that effective technology has not been used for various reasons. One of them are budgetary reasons, as tools are only used in big cities, but police departments are busy doing other things and there is not enough time for training and using the tools. Another reason is bureaucracy, and this speaker mentioned a case where there was a tree blocking the view of a CCTV camera and it took a lot of back-and-forth between different administrative divisions in the city to finally remove the blocking.

The third panellist mentions that data mining and profiling after 9/11 has not been very effective and only serves as a stigmatisation tool, and that the techniques did not prevent other attacks. The fourth person mentions another example where 20 years ago the US National Security Agency (NSA) designed chips to encrypt information, but at the same time installed backdoors. After a lot of controversy the project failed. We are now moving to a new era of binary information and we need effective big data and data mining technologies.

The fifth speaker thinks that the requirements for surveillance technology demanded by the end-users, policy-makers, etc., were not the right ones. This panellist mentions biometric passports, which initially were not accepted by the public, but are now widely used and more or less accepted. Another similar example is the use of microwave imaging in airports. A challenge is that there is little information available to the public at large on how these technologies actually work. The sixth speaker thinks that it is a matter of a solution looking for a problem, and that efficiency is not sufficiently taken into account.

3. What ethical values, principles and ideas – other than privacy and personal data protection – need to taken into consideration in assessing surveillance? Is it ever possible to make an exhaustive list of these values, principles and ideas for each (type) of technology?

The first answer was that the impact on the economy and mistrials are two important things to consider. The second speaker says that surveillance tools are just that: tools, and they do not have values, they have rules, and it is hard to put values in the system. It is the users who need training, respecting the people and keeping in mind that they are fragile in the system.

The third person mentioned that research is currently being conducted about the social cost of surveillance. The fourth person thinks that one important thing to take into account is trust, the system must do what it's supposed to do and users must thrust the authorities. But this trust is built evaluating the system.

The fifth panellist mentioned that persons have the right to integrity, and the task must be carried in a balanced and proportional way. The key is communication and transparency of the system to the users. Another important thing is the risk of false positives. The last panellist says that there must be a protection framework for the users, which includes: legitimacy, proportionality, legality, judicial control, due process, transparency, and accountability.

4. Are the developers of surveillance technologies, policymakers, etc. taking ethics seriously? When it comes to ethics, what each of them is doing good and what each of them is doing bad? Any scope for improvement?

The first panellist argues that developers of the systems and policy makers do not take ethics seriously. The second speaker stated that not many people take privacy seriously and mentioned an example of an event where people were given tracking bands and there were no issues. This person mentioned that data protection is not the same as ethics and people do not understand privacy.

The third panellist says that the situation has changed slightly and there are currently many new projects that are targeted specifically to deal with ethics, but there must be cross-fertilisation of these projects. The fourth researcher argues that "ethics" must be defined first, if it is defined by law then people will take it seriously. The system might have ethic checks but the users could have "low" ethics. Another researcher mentions that from the EU perspective, now it is a requirement to have users of the systems as partners in the projects. The last panellist mentioned that there is a huge difference between ethics and management of ethical issues. As long as you have ethics checklists, you can do almost anything.

5. Questions from the audience

The first question was about how one could get consent from the users in a surveillance system. One of the researchers answered that you must be open about the technology, disclosing the how, the why and by whom. Another speaker thinks that you do not need the public's consent. But when there is resistance to new things, you know something might not be right. The public must participate in the policy-making.

The next question from the public was on how do you get consent from the public to use private tools (like Facebook and Google). Two of the speakers agree that transparency is key. Another speaker adds that people should understand that uploading to social media is subject to surveillance, and the government has starting banning the use of encrypted communications.

The next was a statement saying that ethics are subjective and efforts should be used to first define the ethics. For example, with the creation of research projects “without technology”, i.e. projects that specifically and exclusively deal with ethics, social aspects, politics, etc., of surveillance and not with technology development. One of the panellists answered that social acceptance is a society construct grounded in the interaction of human societies, which are dynamic.

The next question was that the red line, or limit on what can be done, is moving, but the question is how far it can go. One speaker answered that young people are being “radicalised” and some limits will have to be imposed.

The last question was a statement that both sides (both technology and end-users) must continue to challenge each other. If police stops being challenged, this will have unfortunate consequences. One of the speakers complemented by saying that people do not know what ethics mean, but the discussions on this matter nonetheless are healthy.

4 Observations

Although plenty of statements made by the panellists, some of them being of a rather general nature, have been, in one or another way, discussed earlier in, *inter alia*, academic writings as well as political and popular debates, a few of their observations have caught our particular attention. The editors openly claim that the following paragraphs represent an entirely subjective choice.

As the main rationale for engaging with smart surveillance tools, law enforcement agencies (LEAs) claim that they need to obtain knowledge from information, as they need ‘to see a story’. Yet there is ‘too much information’ available and the challenge is putting ‘all these together and correlat[ing] everything to help investigators do the job’. They have confirmed a quite general yet legitimate claim, but this roundtable was a rare occasion to hear a LEA representative claiming that there is a need ‘to find the right balance between finding evidence and protecting privacy’. And further, that there is a need for preventing surveillance tools from misuse, i.e. the need for ‘check and balances’ and for ‘punishing’ those who have abused the system. This reminds us of the Latin adage ‘*quis custodiet ipsos custodes?*’ (‘Who will guard the guards themselves?’) In a similar vein, one LEA representative even claimed all stakeholders ‘should be mindful of long-term effects of surveillance technologies’.

(By contrast, we have attended a similar meeting a few weeks earlier in Brussels, when a LEA representative of one of the EU Member States said, and this is a direct quote, ‘when there is security at stake, there is no privacy’ and this person was convinced it is written so in the laws of that Member State.)

In the same panel, a lot of attention was paid to trust by the population, and the importance of ‘educating the population’ as key notions to a successful, i.e. perhaps socially acceptable, deployment of a surveillance technology. Yet this is paternalistic and authoritarian as it deprives individuals and societies of any choice. Put simply, ‘education’ is a much stronger statement than ‘the provision of information’. In parallel, the representatives of LEA tend to link a greater acceptance of CCTV to the lack of dictatorship in the history of a given country. Such a statement constitutes an argument in a debate, but it cannot be weighted as a major one.

One of the greatest problems confirmed seems to be a difficulty in mutual understanding among stakeholders in the surveillance ‘business’. In this context, the first panel made many statements like ‘regulators do not usually understand technology and policing’, ‘misunderstanding by the public’ and ‘people do not understand privacy’. Perhaps a partial response can be found in the second panel, in which researchers further argued for a greater transparency on how a given technology both works and is used (‘there is no information on how technologies work’ or ‘you must be open about the technology, disclosing the how, they why and by whom’), as this might increase trust in the authorities that employ them. (Yet we acknowledge that the level of transparency has its own legitimate limits.)

The ‘social scientist’ panel started with a statement that ‘ethics are not a static thing’ and that ethics varies ‘by time’, among other factors. What is considered ethical today might not enjoy the same status in the future. In the case of smart surveillance, we see this rather as concepts or products that are considered unethical today might gradually receive ethical acceptance in the future (but rarely the other way around).

Researchers have also pointed out a number of failures and challenges in the surveillance ‘business’. A CCTV camera covered by the growing leaves of a tree, leaving it more or less useless, is perhaps the most trivial example. The researchers mentioned a few further examples of surveillance technologies developed and placed on the market, but that were actually never used due to budgetary problems. Finally, what has struck us the most is the lack of training for the end-users actually operating the tool; or – even simpler – the lack of time to train them. This calls for prudence while deciding whether such a technology should be developed at all.

The editors particularly appreciate that one of the researchers in the second panel claimed that ‘there must be cross-fertilisation’ between ‘technology’ and ‘social science’ projects. There is indeed a need for more such mutual enrichment. Furthermore, we appreciate that the final statement from the audience sought to ‘continue to challenge’, in a mutual manner, those who *surveille* and those who *are surveilled*. Therefore this debate will continue.