Department of Information
Engineering and Computer Science
(DISI)
University of Trento, Italy

INNOVATION AND ENTREPRENEURSHIP
BASICS - AY 2017/2018

Battle Report for battle 3

Security vs Privacy
Robocop vs Human rights

Privacy:
Danish Cheema [196267]
Elisa De Gasperin [197283]
Nicola Gilberti [198739]
Alex Teatini [198022]
Jiarui Xiong [196515]

Security:
Enrico Magnago [186957]
Alaa Salih [196514]
Sridhar Bangalore Venugopal [196506]
Yuping Yan [196513]

1 Introduction

Security and privacy are the most important elements for citizens; they provide a secure environment for people in which they do not have to worry about getting damaged in any way by others. Often this is achieved by negating the freedom and the privacy of individuals, flattening their differences. Both security and privacy have been an important part of our society, but as time goes by science and other aspects of life got more developed, and it completely changed the meaning of security and privacy. Because of development in every field the world has become a global village, where everybody is connected to each other, and it is easy for anyone to attack someone's security or influence with individual's privacy.

In this period of time in which everything is being digitized and the average usage of internet is significantly high, people rely on many different communication channels to exchange information. It is known that all these actions leave information related to the single individual online, thus it becomes more challenging to safeguard from that. In everyday life, we take steps to improve our own security and privacy by following different behaviours like using a strong password on our email accounts or installing alarms and security cams in our houses etc. Having a weak credential or fewer security measures within our environment will lead to damage in many ways. Both security and privacy are a vital thing to be considered to lead a better and peaceful life.

In this work, we will evaluate the benefits of living in a secure environment and the ones obtained by living in a society that ensures privacy. The scenario places us into 2050 where a city is under Robocop's control. This will cover a situation where the machines deployed in Detroit city to serve the public trust, protect the innocent and uphold the law. The problem is whether a new technological solution to the security issue which has a massive impact on the socio-economical structure of the society should be adopted in the whole United States of America or not.

Figure 1: Robot picture (main source: Google)

Robocops are machines which are shaped similar to a human police officer and provide security by enforcing the law using programmed instructions. Robocops can operate round the clock and perform necessary actions. This is allowed by the data which is given to them jointly with precise and clearly defined instructions. These machines will act without the human participation and enforce the law in a strict way without any differentiation among citizens. Thanks to the use of machine learning and artificial intelligence, Robocops are developed, and their service towards society will add an extra feather in technical innovations. The importance and harm of applying them are debated in security and privacy terms. The discussion between security and privacy will focus on the data collection of individual, exchange of data with third party companies, an employment issue, human intervention, Robocops failure indecision. In subsequent sections, this report will discuss the scenario followed by privacy and security views and reconciliation with the conclusion.

On one side the privacy team will try to demonstrate that, individual data is an essential part of society which can't and shouldn't be trade-off under any circumstances. Mass surveillance changes the thinking and mindset of people and makes it difficult to perform day to day tasks. The fact that only organized crimes could be stopped with this system and criminals would find a way to avoid new security measures will be explored. This method can also cause unemployment, not all people employed in Police and legal system, but a lot of them would lose their jobs. The privacy team will extend their argument by stating that Robocops are not safer than ordinary police officers and exposing personal data to companies is harmful.

On the other side, the security team will try to explain this new and innovative system to the public and exhibit its strengths compared to the current policemen system. Through highlighting the significance of security, the team applied themselves to promoting this project and make it adopted by the whole U.S. They highlight how it benefits the entire society in the long run even if the privacy of the citizen will be damaged to a certain extent. The security team will try to show that the cost required by this new service to be effective is less than the value obtained by the citizens as improvement of their quality of life and will show the importance of Robocops and its benefit to the city.

Finally, in this report, we are highlighting security and privacy views and their implications. The privacy team will try to prove on how the security problem could be solved without exploiting the privacy and security team will justify the importance of applying Robocops in the city with the use of individual's private data.

2 Scenario

Assuming that we are in 2050, large developments of technology has made people step into Artificial Intelligence age. In this period, Robot is not only limited to laboratory experiments but also served in all kinds of roles within the society [7]. Robocop system as an experiment conducted in Detroit was quite successful and showed his special cutting edge advantages. However, there are still some limitations related to this experiment, such as it is narrowed in a single city with only a year. Now we are facing the decision to extend this program to the whole U.S. or discard this idea thoroughly.

The experiment result shows crime rate has declined a lot with the effort of robocops. They can respond to crimes much more quickly and enforce laws more strictly comparing with real police officers. But all this has a cost: the personal mobile phones and sensors will send information about all citizens to the city centre to control robocops and dispense justice in a real-time way. Meanwhile, this system does not ask for any fees or taxes from citizens. The city centre will sell these data to make a profit which is used to sustain this project. Companies or other organisations can buy these data and use them for different purposes without imposing any constraints on their usage and without any effective anonymisation. It will post some privacy threats. People are not willing to sell their private information, and they insist it belongs to their human rights.

During the battle preparation we defined some rules. First one is that Robocop is not hackable, because if not there will be big issues in the privacy and the security of the city and the citizens. It is not practical to use a weak and defenceless system to ensure the safety of the whole country. Many vulnerabilities and related problems will occur such as Robocop may be conducted or controlled by evil organisations. Thus, without this constraint, we can not go on with the battle.

The second one is about the security of the data during the permanence in the city. The data are collected by sensors and transmitted directly to the city centre.The city centre has the responsibility to maintain the integrity and the confidentiality of the data. Integrity means that *a system should ensure completeness, accuracy, and absence of unauthorised modifications in all its components* [1]. Meanwhile, the definition of confidentiality is that *a system should ensure that only authorised users access information* [1]. The system can achieve the availability goals which means that *a system should ensure that all system's components are available and operational when they are required by authorised users* [1].

In conclusion, by adopting robocop system, public security can be ensured while personal privacy is damaged. Privacy group advocates putting personal privacy in a priority position while Security group promotes robocops system should still be valid and adopted in the whole U.S.

3 View 1 - Privacy

3.1 Introduction to the main points

The members of the group standing for privacy acted as representatives of the **International Privacy and Civil Rights Association**. As mentioned in the explanation of the scenario, one year after the Government of Detroit started a new security program based on gathering and sale of private data of the citizens in order to use it to prevent crimes in the city, and it is questioned if this system should be expanded to the whole United States. The group's role is to stand against this plan and in the following sections it will be explained why.

First of all, what is privacy? How is it defined? Privacy is the right to be free from secret surveillance and to determine everything about one's personal information. The first publication to mention the concept of privacy as "the right to be alone" was **The Right to Privacy** written by jurist Samuel D. Warren and Louis Brandeis in 1890. It's an almost two centuries old concept which has somehow lost its importance during the last decades. But a right to privacy is also explicitly stated under textbfArticle 12 of the 1948 Universal Declaration of Human Rights [2]:

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

3.2 Waking up people's feeling

The group firmly believed it was necessary to stimulate some questions in the mind of the audience. This was achieved by asking some simple but direct questions like "how would you feel if somebody was watching you?" Surely everyone has some special moments that he would call private in his life. Moments that concern some important matters, are really intimate or would make one feel uncomfortable with an inevitable sense of fear, shame or humiliation if they were public. Examples like being watched while withdrawing money at the ATM, taking a shower or spending time alone with the partner during a romantic dinner or even some intimate moments were used to enforce the antithesis, leading to questioning if the people listening to the speech would be okay with all that.

3.3 False assumptions

There are some common assumptions which are related to this debate. The first is that only bad people have reason to hide their privacy. In the first moment, someone may agree with that. If he is not doing anything wrong, then what's the problem in being monitored?

But if we consider a journalist, an activist or some type of consultant it is evident that he'd want to preserve his privacy in order to have the possibility to keep his works hidden from unwanted eyes. The second is “I don't care if I'm being watched”. Starting with what has already been mentioned above, that would probably make everyone feel uncomfortable when reading it, and everyone also uses passwords to protect all their data and devices. This demonstrates that even if some people don't want to admit it straight away, everyone is at least a bit concerned about his privacy.

3.4 The problems

After the first statements, which went in a more humanistic direction, the group addressed what they saw as the real and actual problems of the program. The first one is **unemployment**. By letting some robots do the peoples jobs, a massive level of unemployment is created, in this case in the police. It's stated that not every police officer will be replaced by a robot, but most would. If we consider New York city, where there are more or less 50.000 people working in the police, even if not everyone would lose their job it's still a massive amount. The unemployment rate is one of the best indicators of the health of the economy and society. High unemployment brings frustration to the consumer due to a loss of income. The idea is that those without a steady income have a greater incentive to commit crimes than those with a regular income, who may have more to lose if caught. After one year it looks like the crime rate has lowered, but in long terms, everything could just end up masking the problem instead of solving it because there is a risk for the opposite result as a consequence of expanding the program.

Within this system, the citizens will end up living in a **glass prison**. Massive surveillance actively affects peoples minds. It gives people the feeling of always being in a mental prison from which they cannot escape and it creates the feeling of being seen as guilty even if innocent. For the mental health of everyone, the government shouldn't give the trust in the people up and rely on machines, but improve the economic system, educate the children to peaceful living and gain hope in humanity back.

There also some other issues that have to be considered. As already told, in one year the crime rate has lowered. But criminals may **find a way to avoid the new security measures**. For example, criminals are getting technological as well. Technology not only facilitates the commission of many existing forms of illegalities but also presents a target for some new ways of lawlessness which are directed at technological products and services themselves. Some technical changes have created entirely new types of crime. At this point, the main question to the audience was: “Are we sure we are going to incentive new forms of crime?”

Furthermore, since the private company could decide to sell the data to everyone, nobody could stop criminals from buying them and using them to their advantage to commit an individual crime. Regarding that, the group also asked how a **private company** could be trusted to buy and manipulate the citizens' private data. The private company will have the right to do anything with the data, which includes publishing or even selling them to the best offer, and this is by far one of the most significant issues of the system.

At last, **the tourism** had also to be taken in consideration while talking about expanding the system to the whole US. It had to be considered how they would be treated and how they would react. The implementation of the security measure would most probably be difficult to apply and have a negative outcome on the tourism for the whole country. And this again would lead to gaps in the economic system and result in more unemployment.

3.5 Suggestions

To conclude, the group stated that they are not that kind of association that just wants to stop new ideas without getting into compromise. The association is not against strengthening the security measures and progress in general, and it is just against the fact that those measures are exaggerated and violate human rights. The main point is that security should be in the balance with privacy instead of destroying it.

After this, the main conditions under which the association could consider an agreement were explained. Those are:

- Let people decide if and what data to get collected from them because this is the main violation of human rights of the program.
- Collect only significant and specific data about the matter. There is no need to know when people are going to the bathroom or when they are having intimate moments of their life. Furthermore, by relying on the newest text comprehension and computer vision algorithms, most of the data surely doesn't need to be collected or analysed in detail.
- Avoid selling the data to a private company, because that's all but secure and unacceptable.

The speech against the new security system was ended with a last strong quote with the hope to awaken awareness in the audience. Based on the romance of George Orwell [3], a wise man once said: "1984 was supposed to be warning, not an instruction manual."

4 View 2 - Security

This section will first describe the proposed **solution** from the security team and then show how it improves not only the **security of the citizens** but also provides the data required in many fields like **research**, **health care** and in general **product design and development**. An objective of this work is to guide in the decision-making process of the reader. This is achieved by explicitly stating what has to be gained and lost for every possibility and what are their consequences. Afterwards, each person will give his own subjective value to each fact and take a personal decision. In our opinion, this is the most logical process to perform any non-trivial choice, especially under an uncertain or ambiguous setting.

In the history of humankind, there has always been the issue of security. In the era of communication, it has gotten worse by giving **new and more powerful technologies to criminals**, among the others. This is the main reason why we have to exploit our technological knowledge to aim for the **best society possible**. This includes solving issues like security and health care.

This section will show how the technological advancement in law enforcement, employed with success the last year in Detroit, solves the security issue and improves the quality of life of all the citizens without imposing any additional tax.

4.1 Solution to the security issue

In the last year in the city of Detroit, we have seen the Robocop system in place. Robots are used to perform law enforcement in a fully automated way. They rely on massive data collection and analysis to be able to predict and avoid the potentially dangerous situation.

This service is provided to all citizens at no additional cost. It finances itself by giving private businesses access to the collected data. Notice that whoever is managing these information has to do that within the boundaries of the law, otherwise, the robots will stop the criminal action.

The results so far are astonishing: the crime rates have never been so low, and the city is always nice and clean. Robots prevented many different crimes, without any harm to the people. Citizens in Detroit can live their life with the certainty of security without any additional cost. This new technology has to lead to an improvement in the equity between different ethnicities, poor and rich people, from the security point of view. These robots allow to finally put law enforcement one step ahead of criminals in the technological race. All of these facts are showing that the robocop system is conductible and provides long-term benefits to our society. Thus, as the designers of this project, we have to introduce it to every citizen of the U.S.A.

4.2 Comparison with human police officers

The United States of America is a country made by people of different ethnicities. Police officers are required to have no racial bias. However, as human beings, they often fall into stereotypes, without even noticing it. Robocops, instead, perform law enforcement only by applying the law without any ethical or racial bias.

Robocops can reduce crime rates effectively as pointed out in our working example in Detroit. In an era in which information technology develops exponentially and in a country where guns and weapons are allowed, we, as citizens, ask for the best personal security system possible. Robocops have the abilities to move faster and respond to crimes quicker than humans. They will not make any mistakes and take the best strategies when put into a dangerous situation. Even if the robot fails to stop the crime, by using the data collected it can identify who performed the offense and arrest him leaving no way of denial or escaping punishment. They are the most efficient law enforcement tool ever built.

The equality in law enforcement provided by the robots that aren't subjected to human feelings or tendencies ensures that no one is above the law despite their social, political or racial status. Another advantage is added by features such as multilingualism and lifetime of service, along with no salaries. As it said in the paper, "the formal content of the training academy is almost exclusively weighted in favour of the more technical aspects of police work" [6]. To train a qualified police officers, a lot of energy and effort are needed to be input inside. Thus, if we replace policemen with robocops, we can save a large number of resources. At the same time, in accordance with class content, this new system shifts the environment of every criminal from an ambiguous or at most uncertain one to one of certainty: they will get caught and they will end up in jail.

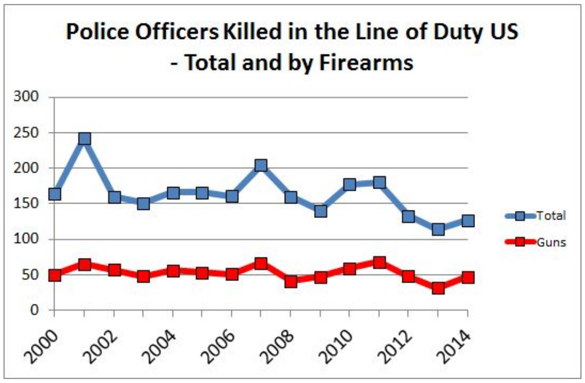

Figure 2: Police officers killed in the line of duty US - Total and by firearms [5]

As is known to everybody, working as police officers is a high risk job. As shown in graph 4.2, the number of police officers killed in the line of duty was more than 100 every year from 2000 to 2014 for many different reasons, some of which are unpredictable. If we replace human police officers with robots, we will save hundreds of lives every year.

4.3 Privacy-security trade off

Our arguing point is the importance of human beings and safety over privacy. Which has more value to us? Privacy or human lives? The fact is that without security, there cannot be privacy. For example, assuming we are in a war-torn country, nobody and no laws can protect our privacy, to achieve that we need a stable and peaceful society. Today we live in a data-domain world. Not sharing information or data contributes to the abstraction of justice. Its very easy to stand with privacy until holding data is directly associated with yourself or the life of one of your loved ones. Lacking data and information is one of the major helping hands in terrorist attacks as well. Some people might exploit the lack of information to hide and shelter. For example, there was a person affected by HIV victim in the UK [4]. He hid the truth and still had sex with a number of men, resulting ten of them to become HIV-positive.

4.4 Final considerations

This new system shifts the environment of every criminal from an ambiguous or at most uncertain one to one of certainty: they will get caught, and they will end up in jail.

Our proposal is an innovative system which is applicable now. From a technological perspective, robocops are currently available, deployable, tested and highly effective in solving the security problem. It is a mature technology and citizens do not have to change their habits, and they can just keep doing what they love to do. Robocops are designed for the future with the ability to tackle future crimes without getting in the way of the population. Moreover, it won't assist only in the security aspect but will also help in data gathering for different fields such as research, health care and any product design and development. All the data someone might need is already there: clean, usable and reliable.

Robocops shows equality indeed. Everyone gets the same service: it doesn't matter if you are a rich person or poor one. Now the only inequality is between Detroit and the rest of the U.S. Robocops in Detroit are a perfect example to illustrate the feasibility of this system, and we hope that the whole United States will experience and enjoy the same welfare we manage to achieve in Detroit.

5 Reconciliation

The city's safety and security are after all our main concerns and all of us despite where we stand we all have its best interest at heart. In the way of achieving what could be said merely as "the best of both worlds" we suggest a midway reconciliation.

The individual data of the citizens which city council collected can be shared with a company on specific criteria. Assuming a system which provides security without violation of privacy, city council requires users data in order to provide protection through robocops. Similar to travel agencies, for example, private data provided by the citizens will be given under consent and not obligatory. In this case, a citizen will provide consent to allow the city council to sell data to companies; more likely to do because of increased regulation on how their data is managed. The data will not be sold or shared between companies for any other external usages. Only the city council is authorized to sell this data and the company which gets the data from city council is the solo user. Data shall be provided to specified companies with a certain objective matter without violating the citizen's privacy under the city council's regulations and compliance to ensure the citizens' privacy not being violated.

The decision of robocops implementation within the city is solely left to the city's council since it is based on certain requirements such as data, sensors and consent. The primary decision shall be made based on the amount of data collected in each city where the robocops are planned to deploy. Specifically lack of data makes the implementation of robocops very difficult, because robocops functionality mainly relay on that personal information of individuals. In a situation where the required amount of data is not in place for deploying the robocops, then a human police officer is assigned in that area to protect the city from crime.

The fear of unemployment is not very high since all human police officers will not be replaced with robocops. In the cities where robocops are not deployed due to a shortage of data, human police officers will continue their job in that city to protect the citizens. There could be many vacancies still occupied by humans when robocops are not in place. However, the recruitment of human police officer could be paused until the city's vision is clear regarding the use of robocops.

During the transition period, both systems will be working hand in hand. Those who are replaced will be moved to other jobs in the same profession. Not to mention, all the new other technical jobs that will be created for IT employees and departments dedicated to the design, manufacture, development and maintenance of robocops.

6 Conclusions

In this report, we have seen how both privacy and security are fundamental to build a wealthier society both from an economical and social point of view. However, as history shows us, It is difficult to reach one objective without negating the other. In the reconciliation part we described a possible solution that allows to keep the best characteristic of both. In this section we try to analyze the consequences that the answer arose from the reconciliation of the two opposite points of view will have.

This new methodology can be seen as a social innovation since it affects all the population equally without any kind of discrimination (economical, racial, ethical, religion, gender) and it has a huge positive impact on their life conditions. This improvement in the short term are limited to better security, a more "legal" society, but in the long term the data collection will speed up the researches and innovations by providing all the data they require. Moreover, as we have seen, it reshapes completely the way people perceive security. If in the previous situation it was ambiguous since a criminal might get away with his actions for a combination of uncontrollable events, with this system in place the environment has moved to a situation of certainty since, as stated in the scenario, robots might fail in preventing some crimes but they will definitely catch the offenders.

From the privacy perspective in the reconciliation the situation for the citizens has improved a lot: there are strong guarantees about how their personal data is going to be handled and their information is not going to be sold to companies without their explicit consent. The city council will have certain conditions in case of selling data to private companies and does make sure that there is no harm to citizens by issuing those data. Additionally, the city will also be benefited with the income which they receive from the companies and those revenues could be used for further developments. However, we think that given the undeniable advantages offered and the most explicit data handling policies most people will give their consent and thus this will not affect the effectiveness of this new technological system.

The introduction of this technology in the daily life of the citizens will have a huge impact on their environment and how they perceive it and thus change their model of the system in which they live. This will also cause major changes on the culture and on the decision making processes that people use. Moreover, people can rely on security as provided and be clear when evaluating different possibilities thus it can associate to each of them with different costs and benefits. In conclusion, citizens will have a better safety on changes which are adopted in the city leading them to a peaceful environment.

References

[1] Y. Cherdantseva, J. Hilton.
A Reference Model of Information Assurance & Security.
2013 International Conference on Availability, Reliability and Security, Regensburg, 2013, pp. 546-555.
doi: 10.1109/ARES.2013.72
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6657288&isnumber=6657192

[2] Article 12, Universal Declaration of Human Rights, 1948.
https://www.un.org/en/universal-declaration-human-rights/

[3] George Orwell *1984*
https://en.wikipedia.org/wiki/Nineteen_Eighty-Four http://www.george-orwell.org/1984/

[4] Daryll Rowe: Police criticised for 'allowing' hairdresser to deliberately spread HIV while free on bail
https://www.independent.co.uk/news/uk/crime/
daryll-rowe-latest-sussex-police-criticised-deliberate-hiv-infections-gay-men-endangered
html

[5] COPS: KILLING AND BEING KILLED
https://psmag.com/news/cops-killing-and-being-killed

[6] Van Maanen, John.
Observations on the making of policemen.
Human organization 32, n. 4 (1973): 407–418

[7] Seeker's Blog
Robocop
http://innovation.disi.unitn.it/iebasics/2017/index.php/2017/10/18/battle-3-security-vs-privacy/