SICSA'17 PhD Conference
Ethical, Social, and Professional Issues Workshop Summary

Boris Mocialov[1], Prof. Nicholas Taylor[1], Jitsai Santaputra[2]

1. Introduction

Ten socio-technical topics had been prepared for the participants to brainstorm and discuss during the workshop, organised at the Scottish Informatics and Computer Science Alliance (SICSA) PhD Conference in Dundee in 2017[3].

1.1. Topics

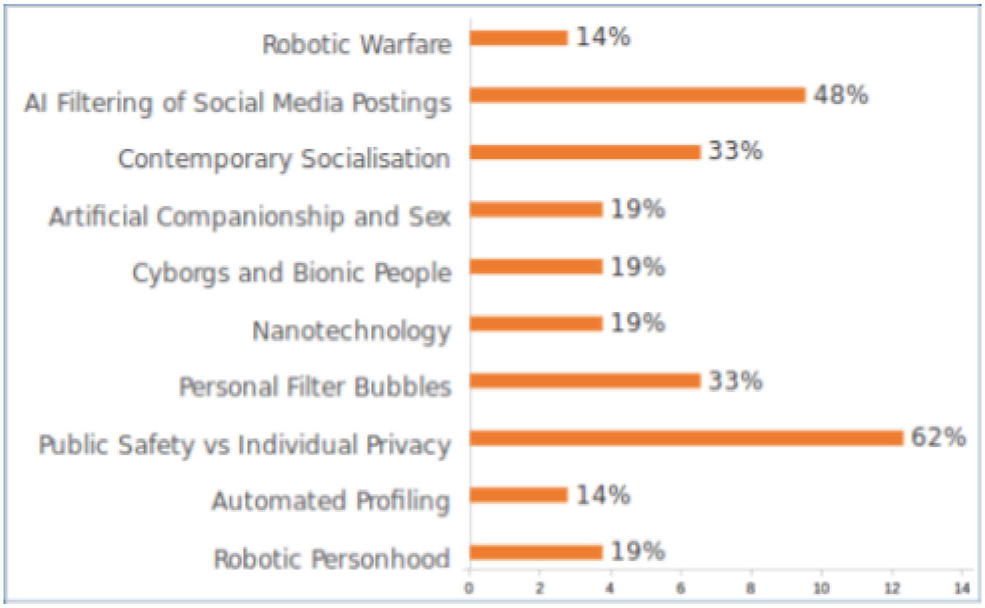

Figure. 1. Topics and the number of responses collected for every topic

[1] School of Mathematical and Computer Sciences and Edinburgh Centre for Robotics, Heriot-Watt University, Edinburgh, UK, {bm4, n.k.taylor}@hw.ac.uk

[2] School of Social and Political Science, University of Edinburgh, Edinburgh, UK, tata211900@hotmail.com

[3] The SICSA PhD Conference 2017 https://www.sutherland.pw/sicsa2017/

Figure 1 lists all the topics that were selected for the participants to choose from before the workshop. Participants were asked to vote on the topics that interest them the most. Online questionnaire had been prepared using the Zoho questionnaires. The participants had been asked to vote on maximum of 3 topics of their interest and answer one question associated with every selected topic. The bars in the figure reflect the interest in a particular topic, accumulated from the amount of people, interested in that topic.

Table 1. Distribution of answers for the pre-workshop online survey questions for every topic

Topic	**Pre-Workshop Online Survey Question**	**Survey Reply Statistics**
Robotic Personhood	Should robots be given rights, so that they could be held accountable for any malicious decision they make against humans or other robots?	50% Yes / 50% No
Automated Profiling	Is the UK’s current guidance that individuals must be able to obtain human intervention adequate protection against the consequences of misclassification?	67% Yes / 33% No
Public Safety vs Individual Privacy	Should the security services be provided with backdoors into end-to-end encryption systems?	69% Yes / 31% No
Personal Filter Bubbles	Should we try to assist like-minded individuals to discover contrary points of view?	100% Yes / 0% No
Nanotechnology	Would it be possible to stop the self-replicating process getting out of hand once the potential for ”grey goo” is detected?	50% Yes / 50% No
Cyborgs and Bionic People	Will such modifications lead to a more unequal society?	50% Yes / 50% No
Artificial Companionship and Sex	Will humans choose artificial companions over real ones?	100% Yes / 0% No
Contemporary Socialisation	Is privacy likely to be taken more seriously by the public in the future?	71% Yes / 29% No
AI Filtering of Social Media Postings	Do we want censorship by AI?	50% Yes / 50% No
Robotic Warfare	Is robotic warfare inevitable?	67% Yes/ 33% No

Table 1 shows questions for each topic. The questions had Yes/No answers to identify the position of the participant on the topic. The questionnaire had been live for approximately one month and participants were notified three times to select their prefered topics for the workshop. After the end of the voting period, twenty one responses had been collected and the final topics were selected based on the number of interests and the equal distribution of opposite views on the questions for each topic. As a result, AI filtering of social media postings, contemporary socialisation, personal filter bubbles, and public safety versus individual privacy have been selected for the workshop.

1.2. Workshop Groups

Participants were grouped together based on their preferred topics. Organisers decided to select four topics for discussion at the workshop based on the level of interest in the topics and a more or less even split on answers to the main question of the topic. Participants were allocated to groups before the workshop with each group including 3 or 4 participants.

2. AI Filtering of Social Media Postings

2.1. Introduction to the topic

AI mining of postings in social media could be used to identify abusive, illegal or misleading ("fake news") content. Mark Zuckerberg appears to be putting his faith in AI to address these issues on Facebook as manual monitoring is clearly not working and almost certainly infeasible. How wise is this? What unintended consequences might arise?

2.2. Pre-Workshop Question

The main question was "Do we want censorship by AI?" During the preliminary stage of dividing into groups, a survey was sent out to find out the participant's attitudes towards the proposed topics. Out of 10 answers: 50% answered Yes while 50% answered No.

2.3. Workshop Questions

In the end, is filtering by AI socially acceptable? Su-bquestions were provided to help stimulate discussions:

i. Is any form of filtering of social media actually acceptable at all?
ii. What about freedom of speech?
iii. Who decides which topics require filtering and which not?
iv. What should be filtered? People, posts, type of content?
v. Is filtering out unacceptable content by AI actually possible?

vi. How “correct” does it need to be for it to be acceptable (Type I and Type II errors)?
vii. What other mechanisms might be used to filter out unacceptable content?

2.4. Discussions

Participants emphasised that they would rather trust a human-being, than a machine, because there is a lack of trust in the machine. Machine filtering of social media postings is inadequate due to the complexity of the rules, associated with the filtering of social media postings. For example, context, attached to the post is crucial in deciding whether the post should be flagged or not. Therefore, flagging of the posts in question by peers using scalar value is more appropriate than automated filtering. While the peer-review could be the solution to the filtering problem, the reviewers must not dictate what should be considered as a standard. Alternatively, purveyors of news could indicate their trusted sources and that other truths are available.

3. Contemporary Socialisation

3.1. Introduction

People are social animals. Being social largely consists of sharing the information within a society. As societies become globalised, sharing is becoming borderless. Social networks, dating, crowdsourcing, and lifestyle applications create a space for exchange of information and meeting like-minded people. There is an apparent demand for much faster and efficient ways of sharing information through hand-held and wearable devices. With the help of contemporary socialisation methods, does it become easier for antisocial individuals to get into contact with other people or do these methods distance them even further?

3.2. Pre-Workshop Question

During the preliminary survey, “Is privacy likely to be taken more seriously by the public in the future?” was asked and out of the 7 answers, 71% said yes and 29% said no

3.3. Workshop Questions

Is privacy likely to be taken more seriously by the public in the future? There were guiding sub-questions provided for the participants to consider:

i) How important will personalisation of services become and how much privacy will people sacrifice to take advantage of it?

ii) Are people likely to prioritise the benefits of location-based services over potential intrusions into their privacy?

iii) How much data from wearable monitoring devices are people likely to disclose and share with others?

iv) Should examples of the potential consequences and regrets of disclosure be more readily available to people?

v) Should services we use remove shared data on request?

3.4. Discussions

Sharing a bit of extra information about ourselves makes our life easier through, for example, targeted advertising, but it also poses threats. Lately, concerns about misused personal data has been increasing, and thus the awareness of privacy has been increasing and will continue to do so. However, it does not mean that the understanding of privacy concerns will rise alongside the concerns themselves. Alertness on behalf of the general public is required to raise the understanding. Who is responsible for protection of personal data, companies or governments? In case if governments would implement policies that would put restrictions on companies on how the data could be stored and used, who would ensure that the policies are being enforced? Users should have the right to be forgotten on request. Unfortunately, it requires additional effort to check whether the requested information has actually been removed and how to enforce the removal on request? What is not sensitive now, may become sensitive later, and what is not sensitive here may be sensitive elsewhere. What we say is what we think and what we believe in. This information is also sensitive and our views may change over time, but what has been shared doesn't disappear.

4. Personal Filter Bubbles

4.1. Introduction

One of the great strengths of the digital world is its ability to bring people together to share ideas and increase social cohesion. Personalisation of systems and services in order to adapt them to a user’s preferences and so avoid inundating them with irrelevant or unwanted content or alerts has obvious benefits. However there is increasing concern that, as like-minded individuals gather together, this personalisation can lead to increased online social separation with users inhabiting “filter bubbles” where points of view contrary to their own do not get presented to them.

4.2. Pre-Workshop Question

The question was posed: “Should we try to assist like-minded individuals to discover contrary points of view?” To which 100% of the seven respondents said yes.

4.3. Workshop questions

During the workshop, the guiding question was “How should we avoid them filter bubbles?” There were sub-questions provided as well:

i) How much are you personally prepared to sacrifice in order to disrupt filter bubbles?
ii) Allowing views that you don’t hold to be introduced to your “timeline”?
iii) Allowing your views to be shared with groups who are unlikely to agree with them?
iv) What other mechanisms could be deployed to disrupt filter bubbles?

4.4. Discussions

Personal filter bubbles could be avoided with the help of the awareness campaigns. One of such campaigns for web browsers “Pop your bubble” could call for the reset of browser data (cookies, history, etc.). The positive side of this campaign would enable anonymous web browsing, while the downside would be the loss of cookies that may act as loyalty cards in the browser and offer cheaper deals to the users. Alternatively, search engines, such as Google, could offer a setting to enable the search for unbiased views. For the user-generated data, service providers could include a “Bubble Pop” button to expose the user to the alternative views or content.

5. Public Safety vs Individual Privacy

5.1. Introduction

There has been much debate recently about the extent to which those charged with protecting the safety of the public should be able to intrude on personal privacy. End-to-end encryption permits secure communication between anybody and everybody. It can therefore be used for good or ill. The so-called “Snooper’s Charter” requires ISPs to maintain records of the IP addresses that their customers access so that the security services can track the connections of persons of interest. The identities of the persons of interest are not known when the records are created so everybody’s connections are recorded. How do we strike a balance between national security and public safety on the one hand and personal privacy on the other? What are the dangers of leaning too far in one direction or the other?

5.2. Pre-Workshop Question

During the survey, the question “Should the security services be provided with backdoors into end-to-end encryption systems?” was posed. Out of 13 respondents, 69% said yes while 31% said no.

5.3. Workshop

Should the security services be provided with backdoors into end-to-end encryption systems? The following sub-questions were provided to stimulate group discussion.

i) How is monitoring justified in a democratic setting?
ii) Should we prioritise cybercrime prevention and national security over personal privacy?
iii) If we need to strike a balance how far should we go?
iv) Should we draw the line at the actual content of communications?
v) What accountability/authorisation mechanisms should be deployed to regulate the security services?

5.4. Discussions

What is exchanged between the user and the service provider is officially agreed upon between the two parties. Users are ignorant or careless of the interactions that happen between the service providers and the third parties. Public safety and individual privacy lie on the opposite sides of a spectrum, it is not binary. The government should be aware of the interactions between the service providers and the third parties and should judge how third parties could use the data, acquired from the service providers. Some data are more sensitive than other data, thus there should be different access permissions for different types of data with different granularities for the same data. When the security is in question, the government should be able to access the user data from the service providers on request. Access to the more sensitive data should require special authorisation (i.e. court warrant).

7. Conclusion

To conclude, each group came up with interesting ideas and even solution for how to deal with particular socio-technical problems. The group brainstorming about AI filtering of social media postings focussed on manual human filtering as a possible step forward towards a more comprehensive filtering system that is less reliant on AI. The group assigned the topic of contemporary socialisation focussed on privacy issues and whose responsibility it is to protect your personal data. The group interested in personal filter bubbles focused on awareness and proposed a concept of erasing preferences/filter bubbles called “bubble popping.” The final group considered public safety versus individual privacy and focussed on necessity of authorisation for intrusions. All in all, the workshop facilitated discussion on four controversial socio-technical topics and the groups were able not only to explore the issues, associated with these topics, but also propose a number of practical resolutions. Further workshops will explore topics in more detail.

8. Acknowledgement

This workshop summary would not have been possible without the main component - the participants, who sacrificed their time and came up with interesting ideas around the selected topics. Individual acknowledgements owed to:
Adisa Akinbode (Glasgow Caledonian University, Glasgow, UK)
Sukanya Benjavanich (Heriot-Watt University, Edinburgh, UK)
Fearn Bishop (University of St Andrews, St Andrews, UK)
Lee Cheatley (University of Dundee, Dundee, UK)
Tom Dalton (University of St Andrews, St Andrews, UK)
Ubong Etuk (University of Glasgow, Glasgow, UK)
Jamie Ferguson (University of Glasgow, Glasgow, UK)
Babalola Kolawole (Glasgow Caledonian University, Glasgow, UK)
Rui Li (University of Edinburgh, Edinburgh, UK)
Oluwafemi Olukoya (University of Glasgow, Glasgow, UK)
Lucy Robertson (University of Dundee, Dundee, UK)
Joanna Rownicka (University of Edinburgh, Edinburgh, UK)
Robbie Simpson (University of Glasgow, Glasgow, UK)
Benjamin Trevett (Heriot-Watt University, Edinburgh, UK)
Katie Watson (Heriot-Watt University, Edinburgh, UK)
Thomas Wright (University of Edinburgh, Edinburgh, UK)
Ryo Yanagida (University of St Andrews, St Andrews, UK)
Ana Ciocarlan (University of Aberdeen, Aberdeen, UK)
Sidi Zhan (University of St Andrews, St Andrews, UK)
Noor Fazilla Abd Yusof (University of Aberdeen, Aberdeen, UK)
Manal Alhathli (University of Aberdeen, Aberdeen, UK)
Linda Lapp (University of Strathclyde, Strathclyde, UK)
Cristina Martin (University of Strathclyde, Strathclyde, UK)
Olumuyiwa Olajuwon (Glasgow Caledonian University, Glasgow, UK)

9. Bibliography

1. Mark Zuckerberg on building global community that is supportive, safe, informed, engaged, and inclusive https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634

2. Facebook Community Standards https://www.facebook.com/communitystandards
3. Applications of Social Networks https://en.wikipedia.org/wiki/Social_networking_service#Application_domains
4. Wearable Facebook https://www.thestreet.com/story/13011778/1/mark-zuckerberg-the-future-of-facebook-will-be-wearable.html
5. Mark Zuckerberg on building global community https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634
6. Personalization and the Filter Bubble https://socialmediaandpolitics.wordpress.com/2013/09/22/personalization-the-filter-bubble/
7. The Tragedy of the Internet https://socialmediaandpolitics.wordpress.com/2013/09/16/the-tragedy-of-the-internet/
8. Investigatory Powers Act 2016 (The “Snooper’s Charter”) https://en.wikipedia.org/wiki/Investigatory_Powers_Act_2016
9. End-to-End Encryption https://en.wikipedia.org/wiki/End-to-end_encryption
10. WhatsApp Messaging https://www.cnet.com/news/uk-wants-access-to-westminster-attackers-whatsapp-messages/
11. FBI-Apple Encryption Dispute https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute