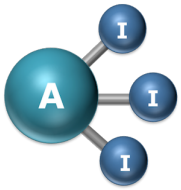

Artificial Intelligence and Augmented Intelligence for Automated Investigations for Scientific Discovery

Re-Coding Black Mirror Workshop
30/01/2019
CPDP 2019 (Computers, Privacy & Data Protection Conference)
Brussels, Belgium

Samantha Kanza
AI3SD Network+

04/04/2019

AI3SD-Event-Series:Report-5

Re-Coding Black Mirror Workshop
AI3SD-Event-Series:Report-5
04/04/2019
DOI: 10.5258/SOTON/P0007
Published by University of Southampton

Network: Artificial Intelligence and Augmented Intelligence for Automated Investigations for Scientific Discovery
This Network+ is EPSRC Funded under Grant No: EP/S000356/1
Principal Investigator: *Professor Jeremy Frey*
Co-Investigator: *Professor Mahesan Niranjan*
Network+ Coordinator: *Dr Samantha Kanza*

Contents

1 Workshop Details

Title	Re-Coding Black Mirror Workshop
Organisers	CPDP Conference Partners
Dates	30/01/2019
Programme	Programme
No. Participants	25
Location	Brussels, Belgium
Organisation / Local Chairs	Pinelopi Troullinou, Mathiew D'Aquin & Ilaria Tiddi
Committee	Full Committee List
Sponsors	Full List of Sponsors

2 Event Summary and Format

The intriguingly named 'Re-Coding Black Mirror' was a one day workshop at the CPDP Conference (Computers, Privacy & Data Protection) which had three main themes of addressing the Ethical and Societal challenges of digital technologies, considering Computer Science solutions against the misuse of technologies, and Technological approaches to prevent Black Mirror's dystopian future. The programme was made up of several sessions of presentations, followed by a group activity to design your own dystopian episode of Black Mirror. These events were all run consecutively so it was possible to attend each talk and take part in the group activities. There was plenty of time for networking as there was both a lunch and drinks session included as part of the day, and there were several coffee breaks.

3 Event Background

This workshop has been run several times now at various conferences since 2017. In 2017 it was run at ISWC (International Semantic Web Conference), in 2018 it was run at WWW (The Web Conference), and in 2019 it was run at CPDP (the specific workshop this report is based on), and will be run later this year at The Web Conference again. Black Mirror (the namesake of this workshop) is a British Science Fiction Series that portrays different dystopian futures that have typically arisen due to a set of digital advancements. Some of the technologies depicted in these episodes do not reflect the current capabilities of todays technology; however there are others that focus on technology quite close to what is available today, and show the concerning potential of the ethical and societal implications of such technologies. In light of that, this workshop was created to create a dialogue between computer scientists, data scientists, social scientists, activists and privacy advocates who all have an interest in the societal and ethical implications of furthering digital technologies, in a bid to ensure that we do not end up living in one of these dystopian futures.

4 Talks

There were six different presentations (as one of the presenters listed in the programme was not present), and each one either related to a specific episode of Black Mirror, or discussed some

of the types of technologies detailed in the different episodes. Each of the presentations was 15 minutes long and questions took place after each presentation.

4.1 "It's not real, but it helps" – Societal and ethical challenges of robotic care technologies - Roger Søraa

Figure 1: Black Mirror. Series 2 Episode 1: Be Right Back - /small`https://www.imdb.com/title/tt2290780/`

This talk focused on the technology from the Black Mirror Episode: Be Right Back which addresses the issues of love between human and robots. The premise of the episode is where a young woman looses her partner Ash and a friend signs her up to a service to stay in touch with the deceased. This begins with her talking on the phone to a synthetic version of Ash, and then progresses to 'the next level' of communication which is a 'real life' Ash robot, which looks, talks and acts like him. There are obviously many ethical and societal implications associated with this notion. and Roger's presentation discusses some of these, with reference to the episode. He discusses the different stages of love: human/human love and the idea of replacing that love with technology to become human/robot love, and the potential resentments that could come alongside that. It is highlighted that this could be the emotional side of love, and that the love between human and robot could potentially take a more platonic form.

The discussions after this presentation raised some other more positive aspects of human/robot interactions, detailing a researcher who had written a book about physical human relations with robots, and how this could be a substitute for humans who have relationship problems or some types of disability; with a more clinical focus on how technology is entering the domain of physical interactions. It was highlighted that perhaps we should consider AI's that are embodied rather than referring to them as robots, as robots is quite an engineering term, and that there are quite clear perceptions of what is and isn't a robot. Roger asked the audience if they would want to replace their loved one with a robot? typically the answer was no but he told us that when he had asked others this question during a similar presentation he had received some more positive responses. There is also the potential of training an AI when you are alive so it is ready when you die, which could make a difference to the accuracy of the AI and how humans close to the trainer feel about the AI.

4.2 Am I talking to a bot or a human? - Transparency in pseudo-AI systems - Claudine Bonneau and Régis Barondeau

This presentation was focused on the transparency (or current lack therof) in AI systems. Pseudo AI systems could refer to systems where humans are providing the computation because the AI is unable to. There are promises about well paid jobs that will be brought about by AI, but behind some current AI systems there are often humans who are training the AI for very limited pay, some about 2 dollars an hour. Using humans in conjunction with AI has brought about a new form of invisible AI, whereby humans are used to train AI systems, validate their outputs, impersonate AI (by answering on behalf of a chatbot when the actual AI can't provide an answer). Often systems are marketed as fully autonomous when in reality they still have a human presence behind the scenes for various eventualities. Some real life examples of this are: spinvox, which uses humans instead of machines to transcribe audio voicemails into text; or Facebook, where 70% of the Facebook Messenger Virtual Assistant requests were handled by human crowdworkers instead of an AI. A big American Tech company used refugees to do algorithmic training for a few dollars a day. The lack of transparency about these types of systems can be confusing for people using systems such as chatbots as they don't know if they are talking to a human or a machine, and typically people tend to change their behaviour, language and response if they know which one they are talking to. Furthermore, exploiting these micro-workers is completely unethical.

The speakers presented a fictional scenario: *Raju is the invisible micro-worker, he is an Indian college student who is paid 2 dollars per hour by an American startup who is commercialising an AI powered digital voice assistant. Raju is paid to pretend to be a chatbot, as the humans are used when the speech recognition engine can't process the instructions. Raju takes over and translates the user requests into text and sends it to the bot. This is near to future, as we have voice assistants now and they will improve in the future, but they can't necessarily understand people with speech impairments or accents. Peter is a user of this application who has had a stroke, and as such he can no longer talk properly. He thinks that a bot is translating his queries but unbeknown to him it is actually a human. Peter the user, is murdering his ex wife, Raju receives vocal instructions that lets him know about his criminal intentions. However, Raju has signed a confidentiality agreement with the company and he doesn't have a specific boss. Raju can either tell someone and be fired or not say anything and be complicit in a crime.*

This example clearly demonstrates why we need **more transparency**. Users have different expectations if they interact with humans or machines. Typically when interacting with machines we are more direct, use specific keywords and avoid being polite. Some humans favour interactions with other humans, perceiving that machines will be unable to help them, and yet conversely some humans actually talk more to machines than a human if they are interacting with a system. Studies have shown that militaries coming back from Afghanistan would talk to a machine more than a psychiatrist. This raised some important questions about the designs of those AIs and related business practices. We need more transparency by design, we need more privacy by design. Human intervention should be clear in the Ts and Cs. Icons could be to demonstrate if you are talking to a human vs machine. Further, is this level of transparency enough? It can't be used to explain or govern such a distributed set of human and non human actors. Humans have limited information and limited power to make choices to change things, and transparency without the power to act is useless. Users need to have a way to meaningfully exercise their choices. There are also cases of 'Technological exceptionalism' - where tech companies don't think that these rules apply to them.

There should be transparency, algorithmic management, limited crowd-workers, autonomy and freedom of choice. There should be a corporate social responsibility to provide acceptable work-

ing conditions, and poor working conditions should not be accepted because our jobs may get replaced by AI. The main discussion point of this presentation was to query if people would be made into second class citizens by a company if their AI could not deal with them. E.g. certain accents are traditionally less well recognised by AI systems. This different level of experience needs to be highlighted! Furthermore, if a company didn't employ humans to deal with their users where an AI couldn't then that in itself could be discriminating against them (albeit potentially unintentionally) and so just removing the human element from this equation isn't necessarily the answer either. Bringing us back around to the point that increased transparency is key.

4.3 Privacy, Security and Trust in the Internet of Neurons - Diego Sempreboni and Luca Viganò

This talk posed the question, what if we had the internet of neurons? What would be the privacy security and trust questions? The internet and computers have progressed vastly since their first conception, from large computers that used to fill an entire room, to ones we can hold in our pockets. With the introduction of the internet of things, everything can now be connected. We could connect to our kettle in a different city so we could have a kettle ready to make tea when we get in. However, if we look forward to the future the internet of things could already be heading towards the past to be replaced by the "Internet of Skills", that involves 5G technology whereby people can connect to everything and also provide skills in real time over the internet. People have already been working on experiments with this technology and it has the capacity to completely change the way we work.

This can link back to technology proposed in Black Mirror whereby the computer could be part of us, part of our bodies; we could essentially become smart humans, or humans 2.0. The presenters proposed a paradigm whereby people can connect to the internet using their brain or perhaps certain devices; which is very interesting from a sociological point of view with respect to fulfilment of democratisation of the internet. This is a huge technology with a huge network and yet it is hard to reach certain areas of the globe, as even if people have computers there still remains the greater issue of how to bring the infrastructure to these hard to reach places such that people can connect to the internet. This technology would confirm some of the existing black mirror episodes, but also bring forward many impossible scenarios. Such as if you connect to the internet then you could become a neuron in the gigantic brain that is the internet. You could synchronise brainwaves with the internet and use them for communication (Brain computer interfaces). Brainwaves could be converted into data.

This sounds like science fiction but it could actually be science. However, this then poses the question of how to encode thoughts But how do you encode instructions, could you transmit packets in the internet of neurons? And how do you receive packets or feedback information from the internet to the brain. This could be done with two different configurations: The first is a bidirectional brain-internet connection with the use of a wearable device (e.g. headphones). This would require protocols between humans and headphones to capture brainwaves, with channels between the headphones and the router to receive the brainwaves translated by the headphones to route to the internet. However, attackers may try to exploit these connections. The second configuration is without headphones for a completely device-less connection, but even removing the headphones leaves two vulnerability points: Location privacy - headset would have a unique ID and if it's on the internet you could be tracked; and authentication issues - how can we protect our brainwaves? Brain print authentication? Thought suppression? At some point we don't need to translate the brainwaves into data but we might be able to transmit them as bi-directional brainwaves with an end vision of a direct connection to the internet (minus router minus headphones).

From a hardware perspective if implants were used there would be the potential for malware issues, and one would expect that something akin to todays modern browser ad block would need to be implemented as a guard against being sent unwanted content. Realistically this isn't entirely different to what is happening today as the younger generation are having their social media presence captured for posterity, they are essentially already translating their thoughts into network packets and sending them out, they are just being transmitted from their brains to a keyboard to a website rather than using a direct link between brain to computer. People are already loosing their filters with respect to what they post online, but what would happen if thoughts were directly posted online? How would you differentiate between what you were thinking and wanted to share versus what are private thoughts? This could be very detrimental for certain people, and Black Mirror hasn't shied away from exploring the negative effects of being subject to a poor public opinion on Social Media (such as their Nosedive Episode which depicts a few simple mistakes leading to a complete nosedive of social media opinion). This raises a whole host of concerns reminiscent of 1984's 'Big Brother is Watching You' and 'Thought Crime'. Could this be used to predict crimes? If people were thinking about intending to commit a crime, or about things that were illegal?

This could give way to a whole new dimension of trust. There could be different ways to generate trust between brains when they are exposed to one another. For example, if something bad happens and another person shows empathy this might generate a level of trust for that person. Or people could set their privacy levels to see friends of friends, with the logic that friends of their friends will have a certain level of trust by association. The narrative of this presentation overall is that in some ways we are already there with a lot of this technology or attempted technology, this would just be another cog in the machine. However, just because this is the case does it mean that it is acceptable? Or is it epistemologically wrong? These are things that we should be engaging further with and considering the privacy and safety aspects of.

4.4 When Thoughts Betray You: Neural Security and the World of "Black Mirror" - Katherine Pratt

Figure 2: Black Mirror. Series 4 Episode 3. Crocodile - https://medium.com/ingenuity-ph/harnessing-memories-the-technology-of-black-mirrors-crocodile-6127387d88ef

The next presentation nicely followed on from the previous one, with a similar topic of exposing people's thoughts to wider society. The concept of mind reading or trying to understand what someone else is thinking has been around for centuries., with humans trying to gain access

to one anothers thoughts. In 1882 the Society for Psychical Research was set up to explore issues such as these. This is a phenomena that has been explored in popular culture such as in Batman Forever; when the Ridder is trying to figure out who Batman is, he invents a 3D television that takes peoples brainwaves, and the person with a bat on their brain is batman. Machines are currently able to steal personal information from human beings such as their bank passwords, so a logical next step would be to see if it's possible to steal deeper information.

This issue is explored in the Black Mirror Episode Crocodile which depicts technology that can be used to recall people's memories. This technology is initially used in an insurance case but ends up implicating one of the witnesses in a murder which leads to a dark spiral of murdering everyone who might have memory recall of this event. Realistically this isn't entirely different to some legal cases that take place today, with lawyers using GPS data from smart watches or recordings from smart assistants (e.g. Amazon Alexa) as evidence in murder cases. However, there isn't currently a bill of rights for thought mining, should there be? There are some other Black Mirror episodes that depict this type of technology, as mentioned in the previous talk, Nosedive depicts social media gone mad (in a way that is chillingly close to todays usage of social media) and Playtest gives a futuristic look into neural video gaming that distorts the reality of the protagonist until he is unable to determine what is real and what is not.

In addition to the concerning consequences of this type of technology, it raises an interesting ethical conundrum of discrimination against people who won't or cannot use technology? If we live in a world where everyone must have an online social profile, what do we do with the people who don't want one? If everyone has implants to allow them to access technology, what happens to the people who say have metal in their body and are unable to do this? Furthermore, what can companies do with the information they harvest from you from these pieces of technology? If this was just about privacy then recording neural signals could be added to GDPR, but it is the interpretation of the neural signals and the use of them afterwards that is the bigger concern.

The interpretation of personal neural information could be vastly incorrect. For example, Vivial Maier, a nanny in the 1950's left behind photographs which were found and displayed after her death. The people who found the photographs made the decision of which photographs to develop and display, and where to put them. But how can we know is this would have reflected what she would have done with them? Just because these people found the information, was it appropriate for them to curate her work? Should it have been given to someone else who was closer to Vivian? Even then would this have had any real reflection on what she would have done? How will artists and historians view this work now that it has been presented by someone else? Following that line of thought, what happens if someone else interprets your neural information? Will it be representative of you?

So how close are we to Crocodile? Amazon is currently selling brain computers, which record muscle signals rather than neural signals, but who knows how these could advance in the future, and what will be done with the information that can be mined from them. Studies are being conducted to obtain information using neural patterns, although currently these seem to be very localised specific experiments. If these do progress what is the implication for society? People are often concerned by what Facebook can do with the data they have about their users, but imagine if they had access to their users brainwaves. They could target adverts to our very thoughts. There are already arguments for why we should be getting off social media and other websites that are deemed untrustworthy, and that people should reflect on their willingness and trust levels towards sharing information with different types of entities. Are there legal precedents to protect us? Laws exist to protect us against certain pieces of information being taken without consent, for example the Biometric Information Privacy Act where fingerprints

cannot be taken without permission; this also covers medical data such as brain scans for medical issues. But would it cover a neural cap for a video game? We would need a much stronger notion of neural security.

Overall this is a concerning view of the future and particularly with respect to the gaming industry, industry backed funding could accelerate the introduction of this technology with companies releasing 'cool' neuro games and subsequently collecting data from them. There needs to be a stronger notion of privacy and personal data protection and legislation.

4.5 Smart Humans... WannaDie? - Diego Sempreboni and Luca Viganò

Figure 3: Black Mirror. Series 4 Episode 2. ArkAngel - https://www.theverge.com/2018/1/8/16864378/black-mirror-arkangel-season-4-jodie-foster-rosemarie-dewitt-review-analysis

This talk focuses on the notion of Smart Humans, and the subsequent concerns that go alongside this concept. We are at a point where Internet of Things devices are everywhere. It is estimated that in 2020 there will be billions of IoT devices online ranging from microwaves, kettles, smart meters, thermostats, lights, shutters, smart fridges, other home and industry appliances, and robots that can make things and teach others to make things. IoT is also highly prevalent in the healthcare industry, smart watches and health devices are extremely popular and there are even smart pacemakers that can be remotely configured. And what to these devices all have in common? They are all connected to the internet!

Since the dawn of time humans have been trying to advance and extend life. This has driven both medical and more recently technological advancements, whereby humans can now make use of artificial pancreas device systems, low invasive pacemakers. robotic prosthetic arms and legs and exoskeletons. These are all fantastic advancements, but what about the security? The Phillips Hue smart lights that can be controlled by a smart phone were one of the first IoT devices to be hacked. Smart Homes have a whole new wealth of attack points that can be utilised without even stepping foot inside the house. Similarly medical devices also have vulnerabilities and entry points. There are various examples of hackers trying to breach these systems, such as the mirai botnet DDoS attack, the WannaCry Ransomware attack. This could lead to the Internet of Ransomware things.

Black Mirror's Arkangel depicts using hardware to control other people. In this instance a concerned mother has well meaning intentions to try and control her daughter when she is young, but her usage of the technology quickly spirals out of control with devastating consequences. This is an extreme but not unrealistic example. Furthermore it's not hard to see

how these well intentioned devices could be subverted to ill intent. Health devices could get hacked, with hackers threatening potentially life altering consequences if their wearers don't pay a ransome. What would happen if the smart in the human was subject to ransom? This could lead to a devastating attack of a new ransomware called 'Wanna Die?'. Hackers could try to extract ransom money by capitalising on the reputation of a previous attack. This could lead to a whole new level of cyber threats that could have a devastating impact on our life and society.

This would require a serious revision of the notions of security and privacy. If we are going to have safe and secure smart humans then we need to build in security from the start. Smart humans require an infrastructure that allows software updates to be applied rapidly to prevent an infection. Humans need a button to turn their internet connection on and off with a strong authentication. Location privacy is hard to achieve if everyone is connected, this would need to be addressed. Furthermore, if everyone was 'smart' this raises charging issues. Is the internet connection free? Who is providing the connection? Wifi? How can I charge them? Wirelessly? What about the people who don't want to be 'smart'? Would interactions between smart humans and smart-less humans change or stop? Would non smart humans accept smart humans? If humans are now smart, at what point do robots become included as a type of humanity?

This raised the question of, if there is a right to be forgotten, is there a right to not be connected? It's hard to buy an unconnected car, the world seems to be going in a direction where soon it will be hard to buy an unconnected toothbrush. We have a perpetual issue of companies collecting our data. Toothbrush companies could collect data about when you are brushing your teeth and sell that data to your dentist. What are they doing to be doing with the data? How do we make sure that the data that is being collected is being collected responsibly. How can we make sure that Facebook is responsibly using our data? Further, there seem to be risks either way, if you are connected you can be hacked, but if you aren't then you lose your digital footprint.In conclusion, we shouldn't have to worry about protecting ourselves because there should be laws and social responsibilities to not do this.

4.6 Academia 4.0: Measuring and Monitoring the Academic Assembly Line - Sven Helmer, David Benjamin Blumenthal and Kathrin Paschen

Figure 4: Black Mirror. Series 3 Episode 1. Nosedive - https://collaborativedialogues.wordpress.com/2017/01/05/nosedive-black-mirror-technologys-influence-on-life-today/

This talk focused on concerns about how academic is monitoring and measuring success. The speakers postulate that metrics are replacing qualitative evaluation and that gamification is

killing motivation, and that there is a real danger that we are turning knowledge workers into robots. The speakers provide a fictitious demo:

Imagine a system where you could choose what you want to optimise: Career, health, fun, benefits, publications etc. Say you choose publications, this could provide suggestions for the best co-authors to boost your publication, suggest a title based on common interests, choose a venue to apply for, auto generate an abstract, provide an expected impact indicator and provide tips of how to move forward with this. If you choose optimise career, this could gamify your career and point towards promotions. Staff could have intranet pages with progress indicators to demonstrate how close they are to their next promotion, they could have ratings and scores and badges as part of this.

This may sound innocent or even fun but our speaker proposes that this is insidious, and looks to take away the purpose of your professional life. People who work in science and medicine etc are typically motivated by the meaning of their work, but numbers and gamification take away that meaning and replace it with something fake, like advancing in a video game or receiving social media likes (such as in Nosedive). This is a dangerous slope and runs the risk of taking away the things that make our life meaningful. Perhaps we shouldn't accept that this is reality? Retain your intrinsic motivation.

4.7 Recode We Must. Bringing ambiguity back in - Tasniem Anwar, Rocco Bellanova and Pieter Lagerwaard

Figure 5: Black Mirror. Series 3 Episode 5. Men Against Fire - `https://www.thebooksmugglers.com/2018/01/five-ways-build-believable-futuristic-military.html/black-mirror-soldiers-against-fire`

This talk looks at the notion of ambiguity, and the idea of re(coding) power and surveillance. The Black Mirror episode referenced in this talk is Men Against Fire which tackles the issues of using technology to dehumanise the enemy in war. The premise of this episode is technology that can be used to make regular humans look like something people are less concerned about killing (in this case mutant zombie-esque creatures who are dubbed 'roaches') to allow soldiers to kill them more effectively and without remorse. This technology is called the MASS brain implant – intelligence (maps, drone, information), sight alteration, memory playback and memory wipe. This implant can manipulate what they know and are going to know. The speakers present three 'codes' for this scenario.

Code 1: George Orwell - Big Brother is Watching You: Power is with the military and they control the MASS system.

Code 2: Foucault Disciplining the Army: The MASS implant helps to discipline the army, the implant changes the soldiers perception to make them more efficient in combat. It alters smell sounds and sights to make killing easier so they don't hear the screams of the victims. This essentially disciplines soldiers to become murder machines. The implant will monitor the soldiers, control their sleep patterns and their dreams, even their entire consciousness, but the soldiers accept this. This implant can be used to discipline the masses, with rewards of nice dreams and disciplinary punishments for bad behaviour. Leaders will have access to this and can survey the army through technology, using passive surveying and active disciplining to make soldiers docile. The governing bodies hunt down zombie mutant figures. Throughout the first half of episode, the roaches aren't seen as humans, but halfway through the episode we discover the zombies are actually human beings. The visuality of how they appear to the soldiers is being controlled by the MASS implant. Using classical Foucault biopower, power over life, these humans become roaches as they have been identified earlier – they have risky diseases, genetic issues or a criminal past and have been categorised as a problem. This shows themes of biopolitics and security and modelling risky populations, where the roaches are being governed, and cut down. This also demonstrates a classical portrayal of surveillance – heretical power of surveillance.

Code 3: Bauman Liquid Power: In this code the power relations are liquid. During the fight, one colleague is seeing a roach and another a human - liquid power. For example, what if we find out that someone else is in charge? But this is automated so we don't know who it is? Power can move with the speed of an electronic signal, and shifts so quickly it is difficult to keep track of it. Therefore it is very hard to know where the accountability and responsibility lies as there are layers of power, and if this power is so liquid and nobody knows where it is situated, how can you hold someone accountable?

Does this in turn all lead back to big brother? At the end of this episode when the soldier is back in the military camp (classical surveillance) the psychiatrist in the army tries to help with the implant glitches, and it turns out he is the real big brother and is in charge of the mass implant and has knowingly brainwashed the soldiers. This soldier gets a choice to relive his military professional life with all the senses and guilt (including actual recollection of killing human beings rather than seeing them as roaches) or have all their memories erased and continue living with MASS. This is a classical surveillance situation, where Big Brother has a button with the power and all of the answers. Is there really one button in the future to stop injustice? We can see how surveillance can be exercised, can power be exercised as one big brother? Or small little brothers through complex systems? Is there just a relationship between the watcher and the watch? What does it mean for responsibility and accountability and moments of injustice? How can we mobilise our resistance against this fluid power?
The speakers recoding suggestion is to recode power and surveillance with the Kaleidoscope. Power is not only liquid it is connected and dynamic; it keeps on shifting. One of the most important things is if you are one of the dots that you are part of the whole, but you only see what is surrounding you so it's hard to find accountability. But you are part of the whole, so we need a framework to think about accountability and responsibility. We need to bring ambiguity back in!

5 Hands on Session

This workshop had a hands on session, which consisted of a telling of a Black Mirror Style story to set the mood, and then a interactive exercise where the participants were split into two groups and asked to script their own episode of Black Mirror.

The first story was entitled 'Schrodingers Man'. The premise of this story is to assume that someone has managed to apply quantum super position to large everyday objects including human beings. If the different "copies" could all synchronise and all collapse into their preferred state (through extended quantum interference), then one could fairly predictably win the lottery, break security systems and do much more. However, what if a couple of the copies decided to revel and not to synchronise anymore? What if they wanted to live their own life? Would they kill the master and all his other slave copies to be free? This raises questions of the notions of identity? What does it mean to be you? The story was called Schrodingers Man as a reference to Schrodingers Cat where the cat is both alive and dead before the box was opened. A similar example would be to take the Ship of Theseus, if you replace all of the planks is it still the same ship? Yes and No. Imagine you saved all the planks taken away and repaired them, those could be used to build another ship, then which one is the ship of Theseus? Who is who? When do the copies have claims to identity? With respect to being able to replicate information indefinitely, at some point we won't be able to distinguish between the copies and the original. This leads to the notion of Schrodingers Attacker, where you can create copies and learn through them. This has consequences for privacy and security. Or Schrodingers Defender. One copy of the defender for each copy of the attacker enrol rebel copies. This postulates very real concerns about the notions of cloning and creating copies of human beings.

After this, the groups departed to script their own episodes of Black Mirror. Interestingly, both groups episodes focused on different types of futuristic transport, one group focusing on bikes and the other on cars. Potentially this is because Black Mirror have yet to produce an episode centred around this type of technology, or perhaps because autonomous vehicles are at the forefront of upcoming technology. Both stories considered dystopian consequences of this technology with respect to control and the divide between those who embrace these new types of technology and those that don't. Although ultimately neither story came to the types of gruesome endings that we have become accustomed to in Black Mirror.

6 Participant Directory

Recoding Black Mirror does not have a participant directory but the list of members and speakers can be found here.

7 Conclusions

Black Mirror provides much food for thought with respect to the future of technology and potential dystopian futures whereby certain aspects of technology turn our world upside down. The talks that were given all had a common trait, that willingly or not we are all becoming part of the net through our work, our bodies and even one day maybe our thoughts. It is hard to know where to put the trust. There are some wonderful things that can be done with enhanced technology but there are also many potential ethical and societal implications, and like Black Mirror these talks served to warn us about the potential issues that could befall us with respect to certain types of technology advancement. Accountability, transparency, responsibility, privacy and security are all measures that need to be taken very seriously with respect to technology and clearly need to br rethought alongside or preferably ahead of some

of these advances to make sure that we don't actually end up in a Black Mirror style dystopian future.

8 Related Events

Recoding Black Mirror has run at the WWW Conference for the last few years. Their other workshop in 2019 can be found here: Recoding Black Mirror Workshop at WWW in San Francisco (13th-14th May 2019).

Upcoming events of interest can be found on the AI3SD website events page.
http://www.ai3sd.org/events/ai3sd-events
http://www.ai3sd.org/events/events-of-interest