vb 2019 LONDON 2 – 4 October 2019

THE PUSH FROM FICTION FOR INCREASED SURVEILLANCE, AND ITS IMPACT ON PRIVACY

Miriam Cihodariu
Heimdal Security, Romania

Andrei Bogdan Brad
Code4Romania, Romania

miriam.cihodariu@gmail.com; andrei.b.brad@gmail.com

ABSTRACT

The angle that we think should be considered in surveillance technology debates is the way in which this type of tech is represented in popular culture. Our hypothesis is that the way security efforts are presented in their fictionalized accounts is actively shaping the way society responds to new technological possibilities.

While society at large tends to push against the use of facial recognition technology and supports the idea of protecting the semblance of privacy and anonymity that we can still enjoy, others are misled by the intensive use of surveillance technology in fiction and believe that these tactics are already approved and running, or that these methods have a greater technological performance than they actually do.

The sources for such misleading imaging can be: any TV show which depicts police dealing with criminality using footage from street cameras; spy movies; cyber warfare in movies or other works of fiction; etc.

Law and media scholars seem to be of the opinion that it's already too late to save privacy. The privacy anxiety and malaise has many important representatives (such as Neil M. Richards & Woodrow Hartzog [1] or Jonathan A Obar & Anne Oeldorf-Hirsch [2]). Others (like Margot Kaminski [3] or Suzanne Barber [4]) are more optimistic about the future of our privacy, or at least try to focus more on how we can protect the privacy we still have and make the data ecosystems more transparent.

It's pretty clear that the development of technology and interconnectedness is making a lot of people uneasy. Privacy is a major source of concern for people living in the digital age. Whether they are right in their suspicions or not, people have even started questioning whether their smart light bulbs are spying on them [5]. The only certainty we have in all of this is that the levels of anxiety regarding interconnectivity, IoT and surveillance are rising.

1. HOW SOCIETY RESPONDS TO SURVEILLANCE TECH DEVELOPMENTS: CURRENT DEBATES

While companies which process huge amounts of personal data are required to account for how this data is used, state actors are not. State actors and other authorities don't answer to a third-party law, since they are the law. Only rarely, due to intense pressure from public reactions, do laws change in favour of citizens and their privacy (such as in the recent anti-facial-surveillance San Francisco win [6]).

But in this process of negotiation with public authorities, members of civil society are often armed only with what they think surveillance is and how they think it works. Depending on the individuals, the level of information they have and its accuracy can vary greatly. We'd like to explore the common misconceptions held by the general public about surveillance and privacy, and how popular culture (through fiction) helps push these opinions and misconceptions one way or the other.

Recent surveys and debates show that, for now, only 45% of Americans [7] say their online privacy is more important than national security. Still, that is almost half the population and the number is rising. Europeans are even more concerned with the privacy of their data, considering that they adopted the all-encompassing data privacy act (GDPR) faster than their US counterparts, and European countries have a longer tradition of being wary of state interference in personal lives (or at least that is the general perception [8] on both sides of the Atlantic). At first glance, the data shows that, while only 45% of Americans value their personal privacy above all else, that number jumps to 70% among Europeans [9]. (In regards to their trust in government in general, outside of private data issues, it seems that the Europeans are more trusting of their governments [10] compared to Americans, though.)

Of course, this doesn't mean that Europe is a safe haven for personal privacy. In fact, it may be that people are more concerned with privacy in Europe precisely because it's under attack a lot more than it is in the US. The NPR reports [11] that the chances of being surveilled are much higher for the regular citizen in the EU than for a citizen in the US, and the growing public outrage regarding the use of facial recognition software by UK police forces point to a worrying level of state information greed, indeed worthy of being compared to a dystopia. When a government minister needs to come out with a defensive statement and insist that the country is 'not a surveillance state' [12], and people still don't believe him, things are definitely amiss.

Are people right to be wary of surveillance? Definitely. It's not just about the more sinister turns this can take if the state can track your every move (like China's disheartening surveillance of the Uyghur population [13]). It's also about data breaches, which are happening so often that people are really starting to understand that they should be careful about with whom they share their data in the first place. With companies, they can just say 'no', thanks to GDPR and similar laws currently being worked on in the US [14]. With public authorities, the right to say 'no' is not a given, and apparently needs to be fought for.

There are some really creative ways of resisting facial recognition software which deserve a special mention. For example, artistic attempts at resisting surveillance [15] by confusing the software with make-up (such as CVDazzle [16]) or with special digital camouflage clothes [17] printed with facial patterns. Unfortunately, no matter how noteworthy these efforts are, their efficiency is bound to be short-lived, since the AI behind facial recognition software continues to learn.

Of course, speaking of the way these algorithms learn detection, there's something profoundly rotten here as well. There are countless reports which indicate that machine learning incorporates the bias of its makers or that of the images which were fed into the algorithm. Thus, facial recognition software is plagued by inherent gender and racial bias [18], making minorities more likely to be targeted for checks [19] and so on. Tech experts are not even sure if a non-biased software can be made [20], let alone whether or not we really need it in the first place. This, in turn, sparks even more controversy, and the problems and unease surrounding surveillance tech don't seem likely to go away any time soon.

2. EXAMPLES OF (INACCURATE) PORTRAYALS OF SURVEILLANCE TECHNOLOGY IN POP CULTURE

There are many notable examples of popular TV and movie theatre fiction which feature mass surveillance in anxiety-inducing ways. We'll present a few just as a palate opener, but the entire list of examples could probably support an entire doctoral thesis.

- **The Wire (2002–2008)**. This show portrays the police's war on drugs, but also features the Baltimore Police Department as being able to spoof cellphone towers and constantly watch its targets. While the portrayal of tech is accurate (so accurate, in fact, that producers were asked to remove some details about how to avoid police surveillance [21]), the popularity of the show definitely contributed to the rise in surveillance-related anxiety. People watched the show and got a first glimpse into how pervasive the surveillance power of the police can be.
- **Person of Interest (2011–2016)**. This TV show depicts law enforcement as constantly operating a machine which spies on every citizen in the US. This machine theoretically serves the purpose of preventing terrorist attacks, but in reality spies on even the most mundane tasks.
- **The Last Enemy (2008)**. This is a short UK series in which the government's extended surveillance leads to race-specific dugs forcibly being used to control sub-collections of the population in a horrifying racist dystopia. If surveillance in the show is able to make the violent targeting of a race possible, it's no wonder that real-world examples which exhibit a racial bias give people cause for concern.
- **Arrow (2012–present)**. In this TV show, hackers are able to continue hacking even though they don't see their screens and have a ping-pong match of sending surges of power back and forth until the computer of one of those involved explodes. Widely considered one of the TV shows which fed most into the bad trope of the 'Hollywood hacker' (as opposed to more realistic portrayals of hacking in *Mr. Robot* [22]), *Arrow* nonetheless made its mark on public perception.
- **Any movie from the last decade's Batman series**. Bruce Wayne doesn't have superpowers, but he has technology – there's nothing supernatural about it though, it's just the regular stuff the police can use as well. That, in a nutshell, is the message behind any *Batman* movie from the recent years, and yet the tech used in the movies is frighteningly efficient. In *The Dark Knight* (2008), a sonar device allows Batman to listen in on every phone call in Gotham and to completely bypass encryption, just like that.
- **Several full-on dystopias such as Equilibrium (2002) and V for Vendetta (2006)**. These feature the extensive use of street and building interior CCTV cameras and the police's ability to instantly be aware of the whereabouts of any citizen at any given time.
- **Several police-related TV shows such as Lucifer, CSI, Bones, etc.** Even when we're looking into a TV show which is sympathetic to police officers as the good guys, the way their technological capabilities are portrayed is inaccurate and fear-inducing. Here are just a few things which fictional police detectives do on these shows and which don't work like that (yet) in real life:
  - Scanning an artistic sketch of someone and the computer immediately coming up with a real identity
  - Instant fingerprint scanning (the police detective uploads it into the computer or takes a photo of the fingerprint with their phone and – bam! – the individual is identified)

- Zooming in and clarifying CCTV images instantly so that a face is clear and recognizable regardless of the distance... for that face to be, again, instantly identified in a database.
- Instant voice identification based on a single short recording (indicating that the police have sufficient data to know how everybody's voice sounds).

Why do we think pop culture portrayals are relevant?

We've seen how surveillance technology is misrepresented in fiction and popular culture. But why would that be relevant to current debates regarding privacy and surveillance, and how can we conclude that the perceptions derived from fiction really do influence individual positioning towards real-life debates?

First and foremost, it's people themselves who opt to use dystopian metaphors as a means of expressing dissent towards new law developments or state practices. Here are just a few examples:

- The machine-learning program created by the NSA to identify terrorists was dubbed 'Skynet' [23] in protest, and the name stuck.
- The Anonymous/Guy Fawkes mask [24], made popular by the film *V for Vendetta*, was used in the 2014 protest against mass surveillance across 15 countries.
- The Stop Watching Us coalition chose the Eye of Sauron (from the mass hit *Lord of the Rings* trilogy) as its logo [25], in protest against mass surveillance techniques.

Also, Alabama's May 2019 anti-abortion law was met with protests in which women donned the specific *Handmaid's Tale* [26] red outfits. While this last example is not necessarily tech-related, it still highlights this overarching trend which demonstrates people's willingness to see dystopian dangers and slippery slopes in the most alarming current developments.

There are also in-depth sociological explanations as to why protesters have increasingly adopted costumes [27] over the past few years: the metaphors conveyed are more powerful and easy to comprehend in a second. Perhaps dystopias are also the go-to narrative for their power of conveying the discontent of protesters through the inherent storytelling and easy-to-comprehend idea.

Secondly, it's not just laypeople: scholars do this as well. Ever since digital landscapes emerged significantly, almost every aspect of life mediated by technology has been compared to a dystopia.

Even scholars who are more optimistic about the transformations of modern life report that people tend to filter contemporary developments through a dystopian lens. Here's a less than exhaustive list of technology-derived things that people have intensely described through dystopian terms:

- Urban privatization (gated communities), as reported by C.P. Pow [28]
- The aggregation of medical data in national data networks [29]
- Localization media [30]
- Artificial intelligence and robotics ([31], to name just one paper of many)
- The Internet viewed as a dystopian instrument of control [32]
- Fertility aid research [33]
- Biometrics and consumer electronics (IoT in a nutshell, as reported by Peter M. Corcoran [34]).

It seems that dystopias in general or particular dystopias have become the go-to whenever recent technological developments are discussed. Also, it's dystopias themselves that have changed, too. More and more, the dystopias of the past 40 to 50 years identify just one culprit as the source of troubles, the moment when things took a turn towards the dystopic state described. That culprit is technological advancement. Just look at some of the recent dystopias which became pop culture phenomena (*I am Legend* and other post-apocalyptic worlds were all ended by a science-fuelled catastrophe, just like every recent zombie movie; *The Hunger Games* and *Divergent* are both about a surveillance-fuelled dystopia enabled by big tech; and so on). If earlier dystopias were casting various causes as the roots of evil, such as dictatorships or magic or personal evil (cannibals, depravity, etc.), recent dystopias all seem to fear the rise of big tech. This could be due to a generalized disenchantment towards science or to various other little causes – one of us has developed the idea in more detail elsewhere [35]. But the fact of the matter remains that technology is increasingly being cast as the villain (or, more accurately, as the enabler of villainous systems).

We can wonder whether the classic dystopian pictures have given rise to people's fears and whether now they are projecting those fears onto tech, or whether the dystopias are simply a convenient metaphor which one can use to express everything that is unsettling about the rise of big tech. In all truth, it's probably a little bit of both, so to ask this question is similar to the never-ending debate on which came first, the chicken or the egg.

We'd like to make one more note regarding this borrowing of dystopia metaphors in current tech debates: by analysing all this, we don't mean to imply that people are wrong to be concerned with surveillance technology or that their wariness is an exaggeration based on the dystopias they're acquainted with. Far from it. On the contrary, we think it's very telling when state-level decision-makers end up having their deeds compared to classic dystopian moves.

Finally, movies and TV shows are not abstract art divorced from social realities. Film has always tapped into public consciousness in order to follow social and cultural history [36] and reflect the main concerns of the day. That's precisely why TV shows and movies in the past decade have increasingly been featuring topics related to mass surveillance, even if the scenario is not new, but a revival of an older sci-fi classic (like the *Electric Dreams* series, based on short stories by Philip K. Dick).

Even police officers themselves admit that fiction creates expectations regarding how the police operates. In an opinion piece [37], police officer Barney Doyle laments that inspiring fictional detectives set the bar too high for real-life police representatives. While we would argue the opposite – namely that portrayals of superior surveillance tech in use by police makes people even more wary of real-life police and their tech than they would otherwise be – his insight is valuable for establishing the connection between fiction and real attitudes towards law enforcement.

The media itself is not shy of comparing the real-life technologies used by police forces with dystopian accounts, such as in this otherwise false claim made by *The Mirror* [38]. Considering all this, we would argue that the two sides (fictional representations of mass surveillance vs. public reaction to actual technological capabilities) are more connected than ever.

3. WHERE THIS ALL LEADS US

It's becoming pretty clear that the Internet, and digitalization in general, are not the freeing tools they once were or which they arguably set out to be. Localization media, surveillance, and the shrinking

anonymity you can enjoy online are transforming the world wide web into a playground for large corporations and state actors looking to keep an eye on people or to change people's minds about something (either in the form of arguably harmless advertising or in subtle and pervasive ways, such as in the *Cambridge Analytica* scandal).

This restriction of the freedoms enjoyed by the average Internet user comes hand in hand with a general fencing-in of the Internet itself. China already has The Great Firewall in place and Russia appears to be trying to follow in its footsteps [39] in order to cut off its population from the rest of the web. These two state actors are the most visible in the recent news, but they are far from alone in restricting Internet use for their citizens. If we take a look at the *Freedom on the Net* reports, between the 2009 report [40] and the 2018 report [41] the number of countries which are judged to have no free Internet jumped from four to 20. Even accounting for the larger number of countries analysed in the report (15 in 2009 and 65 in 2018), that's still a jump from 27% to 31%.

The building of borders online by large decision-makers has come to be known as the balkanization of the Internet (as described by Stefan Tanase [42]). But most of all, states are researching more and more ways to keep tabs on their citizens and residents, in unprecedented ways. The scandals and debates regarding the adoption of facial recognition software, detailed in this paper, seem to be just the tip of the iceberg.

While on a personal level we are as outraged about the indiscriminate use of surveillance technology as the next concerned citizen (and we do think companies and law enforcement representatives should be called to account for how they use our data and how much they infringe on our privacy), we also think that we, the civil society as a whole, should get our facts straight.

As individuals with an interest in anthropology and digital spaces, we may be fascinated by the way popular culture informs, misleads, nurtures outrage or offers powerful metaphors to use for expressing that outrage. But while the misinformation and its spread can be fascinating on an anthropological level, it's in everyone's best interest for people to become more aware of the unrealistic portrayals of surveillance technology that they buy into. We should continue to strive to zoom in on the way our data is used and on the real technologies used to surveil us, while busting the myths introduced by fiction.

And this is where it falls to us and you, as industry representatives and (at least casual) advocates of human digital rights, to be more aware of the intersections between fiction, popular culture and the public perception of surveillance technology. As people working in the industry or connected niches, we're the ones who should have people's backs on this.

REFERENCES

[1] Richards, N.M.; Hartzog, W. Privacy's Trust Gap. 126 Yale Law Journal 1180 (2017). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2899760.

[2] Obar, J.A.; Oeldorf-Hirsch, A. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society. https://www.tandfonline.com/doi/abs/10.1080/1369118X.2018.1486870.

[3] Margot E. Kaminski. http://www.margotkaminski.com/.

[4] Barber, S. Is Privacy Dead? https://identity.utexas.edu/id-experts-blog/is-privacy-dead.

[5] Is your Smart-Bulb Collecting Data? #IoT #SmartDevice. https://blog.adafruit.com/2019/03/10/is-your-smart-bulb-collecting-data-iot-smartdevice/.

[6] McCarthy, K. San Francisco votes no to facial-recognition tech for cops, govt – while its denizens create it. The Register. May 2019. https://www.theregister.co.uk/2019/05/14/san_francisco_facial_recognition_ban/.

[7] The Great Debate: Online Privacy vs. National Security. SaferVPN Blog. https://www.safervpn.com/blog/online-privacy-vs-national-security/.

[8] Wittmeyer, A.P.Q. Do Europeans really care more about privacy than Americans? FP. https://foreignpolicy.com/2013/06/11/do-europeans-really-care-more-about-privacy-than-americans/

[9] Bisson, D. 70% of Europeans Aren't Willing to Sacrifice Privacy for New Services, Survey Reveals. The State of Security. https://www.tripwire.com/state-of-security/security-data-protection/70-europeans-arent-willing-sacrifice-privacy-new-services-survey-reveals/.

[10] Trust in government, policy effectiveness and the governance agenda. https://www.oecd-ilibrary.org/governance/government-at-a-glance-2013/trust-in-government-policy-effectiveness-and-the-governance-agenda_gov_glance-2013-6-en;jsessionid=U5OGOCaolwY7Dv4yn5e07yGn.ip-10-240-5-5.

[11] Gjelten, T. Which Citizens Are Under More Surveillance, U.S. Or European. NPR. https://choice.npr.org/index.html?origin=https://www.npr.org/2013/07/28/206231873/who-spies-more-the-united-states-or-europe.

[12] Corfield, G. UK is 'not a surveillance state' insists minister defending police face recog tech. The Register. May 2019. https://www.theregister.co.uk/2019/05/03/facial_recognition_debate_westminster_hall/.

[13] Cockerell, I. Inside China's Massive Surveillance Operation. Wired. May 2019. https://www.wired.com/story/inside-chinas-massive-surveillance-operation/?mbid=social_twitter_onsiteshare.

[14] Gatlan, S. Bill Introduced to Protect the Privacy Rights of Americans. Bleeping Computer. April 2019. https://www.bleepingcomputer.com/news/security/bill-introduced-to-protect-the-privacy-rights-of-americans/.

[15] Monahan, T. Resisting Surveillance Through Art. National Communication Association. June 2015. https://www.natcom.org/communication-currents/resisting-surveillance-through-art.

[16] CVDazzle. https://cvdazzle.com/.

[17] Heathman, A. Protect your privacy with anti-surveillance clothing. Wired. January 2017. https://www.wired.co.uk/article/anti-surveillance-clothing-adam-harvey.

[18] Vincent, J. Gender and racial bias found in Amazon's facial recognition technology (again). The Verge. January 2019. https://www.theverge.com/2019/1/25/18197137/amazon-rekognition-facial-recognition-bias-race-gender.

[19] Simpson, L. Black women are far more likely to get stopped and searched by airport security as TSA scanners are 'triggered by their hair'. Mail Online. April 2019.

https://www.dailymail.co.uk/news/article-6936327/Black-women-likely-stopped-searched-airport-security-hair.html.

[20] Fussel, S. Can We Make Non-Racist Face Recognition? Gizmodo. July 2018. https://gizmodo.com/can-we-make-non-racist-face-recognition-1827639249.

[21] D'Orazio, D. Creators of The Wire were asked to remove details that could help criminals avoid wiretaps. The Verge. April 2015. https://www.theverge.com/2015/4/12/8395529/the-wire-was-asked-to-remove-details-about-avoiding-wiretaps.

[22] Doctorow, C. Mr. Robot Killed the Hollywood Hacker. MIT Technology Review. December 2016. https://www.technologyreview.com/s/603045/mr-robot-killed-the-hollywood-hacker/.

[23] Grothott, C.; Porup, J.M. The NSA's SKYNET program may be killing thousands of innocent people. Ars Technica. February 2016. https://arstechnica.com/information-technology/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people/3/.

[24] Protesters rally for 'the day we fight back' against mass surveillance. The Guardian. February 2014. https://www.theguardian.com/world/2014/feb/11/day-fight-back-protest-nsa-mass-surveillance.

[25] Burrington, I. The Eye of Sauron on the streets of D.C. Waging Nonviolence. October 2013. https://wagingnonviolence.org/2013/10/stop-watching-us-sauron/.

[26] Parham, J. Depth of field: in Alabama, The Handmaid's Tale is a haunting metaphor. Wired. May 2019. https://www.wired.com/story/depth-of-field-alabama-handmaids/.

[27] Velocci, C. Why Protesters Love Costumes. Racked. March 2018. https://www.racked.com/2018/3/2/17042504/protest-costumes.

[28] Pow, C.P. Urban dystopia and epistemologies of hope. https://journals.sagepub.com/doi/abs/10.1177/0309132514544805.

[29] Davies, S. Dystopia on the Health Superhighway. The Information Society. https://www.tandfonline.com/doi/abs/10.1080/019722496129800.

[30] Hemment, D. The locative dystopia. https://eprints.lancs.ac.uk/id/eprint/30831/.

[31] Berg, A.; Buffie, E.F.; Zanna, L-F. Should we fear the robot revolution? (The correct answer is yes). https://www.sciencedirect.com/science/article/abs/pii/S0304393218302204.

[32] Hetland, P. https://www.degruyter.com/downloadpdf/j/nor.2012.33.issue-2/nor-2013-0010/nor-2013-0010.pdf.

[33] Roberts, D.E. Race, Gender, and Genetic Technologies: A New Reproductive Dystopia? Signs Journal of Women in Culture and Society. Volume 34 no. 4. 2009. https://www.journals.uchicago.edu/doi/abs/10.1086/597132.

[34] Corcoran, P.M. Biometrics and Consumer Electronics: A Brave New World or the Road to Dystopia? [Soapbox]. https://ieeexplore.ieee.org/abstract/document/6490479.

[35] Cihodariu, M. Ph.D. Thesis, University of Bucharest, 2014.

[36] Film as social and cultural history. History Matters. http://historymatters.gmu.edu/mse/film/socialhist.html.

[37] Doyle, B. How fictional characters influence people's perception of police investigations. PoliceOne.com. July 2016. https://www.policeone.com/csi-forensics/articles/194966006-How-fictional-characters-influence-peoples-perception-of-police-investigations/.

[38] Aspinall, A. Minority Report-style facial recognition technology to be used on fans at Champions League final. The Mirror. May 2017. https://www.mirror.co.uk/news/uk-news/facial-recognition-technology-used-champions-10476768.

[39] Meyer, D. Putin signs Runet law to cut Russia's internet off from rest of world. ZDNet. May 2019. https://www.zdnet.com/article/putin-signs-runet-law-to-cut-russias-internet-off-from-rest-of-world/.

[40] Freedom on the Net. A Global Assessment of Internet and Digital Media. April 2009. https://freedomhouse.org/sites/default/files/Freedom%20OnThe%20Net_Full%20Report.pdf.

[41] Freedom on the Net 2018. https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.

[42] Tanase, S. Internet Balkanization: why are we raising borders online? Virus Bulletin. 2018. https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Tanase.pdf.