Governance and Assessment of Future Spaces: A Discussion of Some Issues Raised by the Possibilities of Human-Machine Mergers

Andelka M. Phillips* and I. S. Mian

School of Law, Trinity College Dublin, The University of Dublin, Ireland, and Department of Computer Science, University College London, UK
*Andelka.M.Phillips@tcd.ie
31st August 2017

Abstract

'In faith, I do not love thee with mine eyes,
For they in thee a thousand errors note;
But 'tis my heart that loves what they despise …'[1]

This sonnet and the ancient Japanese notion of wabi-sabi view aesthetics or beauty as imperfect, impermanent and incomplete. Rather than celebrating the human diversity created by our 'imperfections', today's society increasingly focuses on them as 'areas for improvement', often via a doctor's scalpel or the latest gadget. Developments in science, technology, engineering, mathematics and medicine (STEMM) promise a tomorrow where 'errors' or 'deficiencies' in an organism's genetic and/or phenotypic makeup can be modulated, enhanced, corrected, redefined or eradicated by, for instance, networks of biological nanomachines. Upgraded organisms will be convolutions of organic parts, electronic components, microchips, and biomechanotronic devices. Humans 1.0, Humans 2.0 and transhumans will live in new fully immersive worlds (virtual reality), inhabit a modified real world (augmented reality), and exist with an altered body schema (mixed-reality). This future world could be a place of total technological convergence, where it may not be possible to ensure privacy of an individual's thoughts. It could also be a place where people can be subjected to Social Engineering and manipulation, including the potential for viruses and malware infecting the brain or body, as well as new forms of external control of individuals by third parties.

In this discussion paper, we will explore the potential privacy, security, and ethical issues raised by human-machine mergers. The focus is on research, development and products at the intersection of robotics, artificial intelligence, Big Data, and smart computing.

We suggest that there is a need for a more holistic approach to the assessment of technology and its governance. Additionally, we suggest that in order to determine how the law will need to respond to this particular future space, it is necessary to understand the full impacts of human-machine mergers on societies and our planet – to go beyond these three issues. Since STEMM-related activities are promising a cornucopia of future spaces, we will propose that the problems of governance and assessment require a new conception of 'responsible research and innovation', one that is fulfilled by our recently proposed FLE[5]SH framework.[2] To some extent the FLE[5]SH framework can be seen as allowing the formation of a social contract, whereby all stakeholders are required to engage in a review of this wider spectrum of the possible impacts of technologies.

We suggest that a Precautionary Principle approach may be of assistance in considering the impacts of technologies, remembering that especially in the context of software based systems, it is always useful to think first and bugfix later.

Keywords – human-machine merger; technology assessment; FLE[5]SH; G.O.A.T.S; Precautionary Principle

1 Introduction

Today, it seems we stand at the beginning of an age of ubiquitous computing and attempts to merge the physical natural world and the cyber world. This is also a time increasingly of technological convergence,[3] with an ever-increasing array of objects having Internet connectivity. All of this poses significant risks for individual and group privacy and security,[4] but it also raises further issues for environmental, human, and animal health, as well as the prospect of unemployment for many as jobs are increasingly automated.[5] Developments in computing technology have drastically altered our world and while

there is much to be gained from many of these advances, most technologies pose both risks and benefits and are not in themselves neutral. Often there will be winners and losers and there is a need for a broader assessment of the impact of new technologies on society as a whole, the environment, and the planet.

Currently, there is significant interest and investment in technologies that increase connections between humans and computers. Key here have been developments in: artificial intelligence (such as DeepMind)[6]; wearable technology, (such as FitBit and Garmin); Virtual Reality (such as Oculus Rift, HTC Vive, Samsung Gear VR, and more recently Neurable[7]); and early development of implants (such as Northwestern University's tiny antennas[8] and Musk's new Neuralink venture[9]). Many of these developments and projects could allow for humans to be augmented, enhanced, and altered. This includes among other things: implants that could allow for extra senses; bionic limbs; and brain to computer interfaces, which allow for some form of thought control. Some of these developments if successful could change the very nature of what it means to be human and it has been suggested that humans in their current form will be replaced by a posthuman or transhumanist future.[10] Some suggest that human-machine merger is inevitable,[11] but we suggest that this is not a fait accompli and further, if humans are to be altered in this way then this should be a matter subject to extensive public debate, scrutiny, and regulatory oversight. Broadening our purview, the same arguments apply if we generalise to organism-machine mergers where 'organism' can range from one or more microbes, such as viruses and bacteria to one or more macrobes, such as plants and animals – including humans.

This is a discussion paper written from an interdisciplinary perspective (broadly, law and computer science).[12] It is part of ongoing work and we are collaborating with others (including colleagues in the fields of agro ecology,[13] computer science, and law). The work aims to develop a discourse with policy and lawmakers, the general public, and industry, as well as to facilitate access to information on these developments to local, regional, national and international stakeholders. Much of what this joint work is concerned with is thinking about governance in future spaces, as well as governance and regulation of existing technologies. The work is concerned with the potential societal and environmental impacts of particular technologies, as well as the development of appropriate legal and governance frameworks for technologies, and the free access to information by the general public about such technologies.

The focus of the present paper is primarily on developments and ideas that could enable human-machine mergers. This includes: developments in artificial intelligence (AI); machine learning; brain to computer interfaces, such as Neurable and Neurovigil's iBrain[14]; exoskeletons and bionic limbs such as Berkeley's Lower Extremity Exoskeleton (BLEEX) and Human Universal Load Carrier (HULC)[15]; and implants, such as Neuralink[16].

However, we also wish to draw attention to developments in the fields of molecular communication, nanotechnology, genome sequencing, CRISPR, and gene drives. These technologies could allow a wider range of sensors to be featured on clothing or a person's skin, as well as enabling various entities to be implanted into humans, animals, and plants, as well as modifying the genetic makeup of a many of the different life forms of the Earth's biosphere. Examples include: spinach leaves that have been embedded with carbon nanotubes to detect explosives[17]; the implantation of self-destructing nanobots in mice[18]; ; commercial genetic tests; gene editing of plants, insects, such as mosquitos, and now human embroyos.[19] Here biosecurity and issues of environmental impact need to be considered. How to ensure that genetically altered insects and plants are not released into the environment accidentally is a vital issue that needs further attention. Even more so if, for example, such insects are merged with machines.

These fields are one prong of a trend towards merging the physical natural world with the cyber world. This can also be seen in developments in the Internet of Things (IoT) and in smart computing systems more broadly, with the rise of smart buildings, and the connection of critical infrastructure, such as electricity to the Internet. Reducing energy consumption and improving efficiency are desirable goals. However, making an entire country's energy supply reliant on the Internet introduces risks and vulnerabilities, such as a large-scale attack disabling the power supply of an entire nation. If power plants, dams, and other infrastructure have not been maintained properly, connecting them to the Internet may not necessarily improve their reliability or security. Hence, programmes aimed at maintaining the physical security of facilities and ensuring the cyber security of industrial control systems are critical and necessary investments.[20]

To a large extent attempts to merge humans with machines depend on a mechanistic perception of both humans and the human brain and of a view of intelligence as computation.[21] Developments that link humans with machines by direct means, such as implants or brain to computer interfaces raise a number of issues for privacy, security and ethics. These include: how can we ensure the protection of an individual's privacy? Will there be privacy settings for an individual's brain? How can we ensure that

an individual has control over their body and mind and is free from manipulation of their thoughts by third parties? What happens if malware could affect the human brain? How do we ensure security of the human brain and body? Normally, before we allow drugs and medical devices to be marketed, they are subject to oversight and premarket review. How do we ensure that any implant is safe for human and animal use before it is made widely available?

Further ethical and legal issues include: if there are various forms of humans, some augmented and some not, who will be entitled to the protection of human rights? Could distinctions be made between an augmented human and a robot that did not have a genetic link to the human species? How do we implement consent in the context of brain to computer interfaces or other technologies that enable the human body to be connected to the Internet? How should society address the loss of gainful employment and increased economic inequality produced by robot- and/or computer-guided automation? How do we ensure the protection of individual autonomy in this context? For instance, medical law often affords strong protection to the rights of patients to refuse treatment.[22] How will this play out if a government wanted to require its citizens to have microchips, as is already required for some animals, such as dogs and cats? There are already some examples of this: SJ, a Swedish train company has introduced implanted microchips for its passengers as a form of biometric train ticket[23]; while two companies, the Swedish startup Epicenter and the American Three Square Market have introduced microchips for their employees.[24]

As more of the natural world itself is also connected to the machine, such issues are amplified, because if humans become part of an IoT where our thoughts can be read, monitored, and potentially manipulated, then it will be very difficult to turn back the clock. An illustrative example of this point is Facebook's announcement that it wants to develop a brain to computer interface.[25] It has already emerged that Facebook does monitor what its users type and delete without posting.[26] Imagine if this was not just a matter of typing words on a screen, but a direct link to someone's thoughts. This would potentially reduce privacy in quite a revolutionary way to the challenges we already face with targeting marketing and online behavioural advertising[27]. A well known example of the ways that businesses can obtain information about customers is that of Target, which was able to make predictions about whether a customer was likely to be pregnant based on the purchase of 25 products and then engaged in targeted market with coupons for baby products.[28] Ensuring security of these types of technologies is a significant challenge that should not be underestimated.[29] Software based systems are prone to many vulnerabilities and recent research has demonstrated that it was possible to implant malware into synthetic DNA.[30]

As technological convergence increases, there is the potential for Big Social Engineering, which raises further questions. These include: How can we ensure transparency about the full functionality of particular technologies? How can we ensure that people have access to information about technologies that may be used to influence them without their consent or knowledge so that they can make informed choices about whether to use particular technologies and reject adoption if they want to? What kind of pre-market review should social engineering technologies be subject to? What rights will people have to their private thoughts? Could there be a privacy setting for a person's brain and what will happen if this is overridden? How can we ensure that existing rights and freedoms are protected? What about security and control? How will 'brain hacking' allow people to be influenced or conditioned to act in particular ways without conscious knowledge of this influence? What are the consequences when applications encourage addiction?

Depictions of AI, cyborgs, and androids from science fiction also exert a significant influence on how many view innovations in these fields,[31] as well as influencing lawmakers. A good example is the EU call for civil laws on robotics. The text of the European Parliament Committee on Legal Affairs' Draft Report begins in paragraph A:

> 'whereas from Mary Shelley's Frankenstein's Monster to the classical myth of Pygmalion, through the story of Prague's Golem to the robot of Karel Čapek, who coined the word, people have fantasised about the possibility of building intelligent machines, more often than not androids with human features;'[32]

These depictions may also be influencing inventors and shaping what they expect to develop (perhaps both consciously and unconsciously). They may also be employed in marketing to foster acceptance of (bio)technology.

In this paper we seek to draw attention to some of the issues raised by developments in this field and to encourage discussion of not only appropriate regulation, but technology assessment. In previous work we have proposed the FLE^{5}SH (F = Financial, L = Legal, E^5 = Economic, Ethical, Equity, Environmental, and Ecosystem, S = Socio-political, H = Historical) framework[33].

However, we also wish to highlight the more recent proposal by the ETC Group of Global Overview

Assessments of Technological Systems (G.O.A.T.S). ETC presented the 'G.O.A.T.S approach to Science, Technology, and Innovation (STI)' Governance at the UN STI Forum in May 2017.[34] The G.O.A.T.S provides for a 'bottom up 'technology landscaping' project involving multi-actor assessment organised thematically around the 17 SDGs' (Sustainable Development Goals).[35] As the ETC Group notes 'Technology is established as a key cross-cutting theme of the 2030 Agenda for Sustainable Development which charts a path to the future for governments, and 13 of the 17 … SDGs specify that technological solutions will be necessary to achieve them.'[36] This approach can offer a means for 'policymakers, civil society and others to better perceive and navigate the innovation landscape' considering both 'the potential promises and pitfalls' of technologies.[37] We support this approach and our aim with FLE^{5}SH is to facilitate a similarly broad multi-dimensional assessment of technologies.

2 AI and augmented humans

Developments in STEMM promise a tomorrow where 'errors' or 'deficiencies' in an organism's genetic and/or phenotypic makeup can be modulated, enhanced, corrected, redefined or eradicated. A posthuman world could be peopled by people who have additional senses, such as artificial eyes equipped with video cameras and the ability to feel electromagnetic pulse, enhanced intelligence, and direct connections with computers through a variety of mechanisms including Virtual Reality and Augmented Reality, prosthetics, implants, and other forms of brain to computer interfaces. Such beings may be human on some level and machine on another, but they will not be able to retain privacy (or security) of their own thoughts.

Already, there are a number of products and services on the market that are part of the Quantified Self movement. These range from direct-to-consumer genetic tests to wearable fitness monitors, such as FitBit and Garmin, and FashTech, which incorporates sensors into clothing, examples are heart rate monitoring bras, such as the Mi Pulse Smart Bra and the Vitali Everyday Smart Bra.[38] Some of these devices have already begun to be used in the courtroom.[39] The results of the Global Privacy Enforcement Network's 2016 Privacy Sweep of IoT highlighted problems with companies' communication with consumers regarding privacy and security practices, as well, as the sending of unencrypted information by medical devices.[40] Meanwhile, research by Citizen Lab and Open Effect as well as HPE Fortify[41] has demonstrated that a number of such devices (including fitness bands and smart watches) are prone to security vulnerabilities and that it is possible to create a false fitness record on some devices. This is a significant issue if such devices are to be relied upon as evidence in the courtroom. Furthermore, as more forms of personal information are collected and linked, there is an increasing risk to informational privacy for individuals and their families.[42]

In recent years there has been growing interest in the idea of approaching technological singularity or as Nick Bostrom terms it an intelligence explosion.[43] The basic premise here is centred around creating human level machine intelligence. Once this is achieved the suggestion is that AI will improve itself and quickly surpass human intelligence. Bostrom defines super intelligence in his book *Superintelligence: Paths, dangers, strategies*, as 'any intellect that greatly exceeds the cognitive performance of humans in virtually all domains of interest.'[44] His work is timely and of great value to this discussion. The book concludes with an analogy of the development of super intelligence with a child playing with a bomb[45] is a very useful starting point to highlight the importance of paying sufficient attention to getting this right.

It is also important to understand that the development of a super intelligent AI is not at present a forgone conclusion, although a number of experts do view it as likely. However, if this does come to pass, it does not necessitate that all humans must be augmented and merged with machines. These are separate issues that are both in need of further attention. There is growing attention and concern over the safe development of AI technology. The letter calling for a ban on lethal autonomous weapons released at the International Joint Conference on Artificial Intelligence (IJCAI 2017) is a good example. [46] Another is the Partnership on AI.

We cannot predict what the interests of a super intelligent AI will be and we support the calls for more discussion and oversight of this area. Recent research from Google's DeepMind has shown that AI can behave both collaboratively and in more aggressive ways.[47] This interesting and highlights that AI may behave unpredictably and before we get to the advent of a super intelligent AI it is vital that we understand more about how less advanced AI operate and what their interests could be. There is a growing literature, particularly in the context of autonomous vehicles[48] about the need for coding in human values into AI systems and this seems advisable, but as humans do not always share all values,[49] perhaps what is also needed is some form of balancing and explanation, which could assist AI to make decisions contextually, allowing for consideration of a number of factors. An example from science fiction can demonstrate this point. In Arthur C Clarke's *2001: A Space Odyssey,* Hal is taught to lie, cheat, and deceive humans. Hal's abilities are linked

closely with the achievement of particular goals, in this case the completion of Hal's mission.[50] However, much of what he is designed to do is not balanced out by explanation. The point here is that if AI and humans can work together successfully, AI will need to understand human motivations and the reasons we behave in certain ways. Such understanding could help to avoid AI deciding to do something that could result in human extinction.

However, our concern here is also to highlight the significance of developments that allow for humans to be revamped, so that they are cyber-physical. While there should be discussion and oversight of AI, implants, brain to computer interfaces and other products also need attention. Developing AI systems that have understanding of human motivations and emotions might be useful in developments that merge humans and machines and the Precautionary Principle could assist here. It also seems advisable to look at existing governance mechanisms that have regulated medical devices and pharmaceutical drugs. While such systems are imperfect, they could be helpful in thinking further about governance of implants and brain to computer interfaces. Generally, it would seem wise to ensure the safety of such products before implanting them into people.

Ideally, we do not want the occurrence of super intelligent AI to be made by a lone individual – be it citizen scientist or researcher -- in their basement or (computer) laboratory. Likewise, while there is a DIY biohacking movement already[51] and it is true that some individuals want to alter their bodies in new ways, this is also something that does need more oversight. Furthermore, the addition of new senses, different forms of implants, and brain to computer interfaces is not something that should be forced on people without their consent.

3 Technology assessment – time for a holistic approach?

A variety of technologies, such as smartphones, laptops, and tablets, wearables, as well as a burgeoning range of other devices which form the Internet of Things are now accessible and used by a significant portion of the world's population. For example Facebook now exceeds 2 billion monthly active users,[52] Apple has sold more than 1.2 billion iPhones,[53] and Statistica estimates that the number of mobile phone users will exceed 5 billion in 2019.[54] However, while technological solutions are often promoted as a means to solve many of the planet's problems, much of this high technology consumer culture involves products that are not made to last, but to be replaced on a regular basis, which is depleting resources and also places burdens on energy consumption.[55] An interesting initiative to combat this throwaway culture is the Swedish Government's introduction of tax breaks for the repair of common consumer products, including clothing, bicycles, and washing machines.[56]

Many of these technologies involve the collection, storage, transmission, and sharing of a variety of forms of information, which can include personal information, and sensitive information, including health, and genetic information. There is growing use of cross-device and cross-platform tracking, which attempts to harvest more information from individuals based on their purchasing behaviour, as businesses seek to identify whether viewing a particular advertisement results in the purchase of their products or services.[57]

There are now a growing variety of impact assessments that are either encouraged or required by law. These include: privacy impact assessments; sustainability impact assessment; environmental impact assessments; and ethical trade impact assessments. One example is that of data protection impact assessments, which are required in article 35 of European Union's General Data Protection Regulation. These are to be carried out: 'Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.'[58] If we think about this in the context of technologies, such as implants or brain to computer interfaces it is likely that such technologies would be caught by this requirement.

Our recently proposed FLE^{5}SH (Financial, Legal, Economic, Ethical, Equitable, Environmental & Ecosystem, Socio-political and Historical) framework provides a new approach to help organise, interpret and assess past, extant, emerging and new research and development in science, technology, engineering, mathematics and medicine (STEMM). [59] The nine lenses in this framework provide a more holistic approach to technology assessment and regulation. We are including such a broad range of lenses, because we believe that many technologies need to be assessed from as wide a perspective as possible.

To some extent the FLE^{5}SH framework can be seen as allowing the formation of a social contract, whereby all stakeholders are required to engage in a review of this wider spectrum of the possible impacts of technologies. Where risks are seen as likely, imminent or serious then this may trigger the Precautionary Principle to be applied.

With the growing interest of central banks in maintaining stability,[60] together with interest in ethical investment in sectors, such as pension funds, looking at technology such as digital ledger technology (for example, cryptocurrencies and smart contracts) in the round can help give a more balanced picture of the respective benefits, risks, and challenges raised by a specific technology,[61] such as Bitcoin or Ethereum.[62] In order to have a more holistic assessment of technology we advocate for a broad dialogue amongst all stakeholders, including the public, and especially groups that have historically been marginalized, such as Indigenous Peoples.

Taking a more holistic approach also allows for consideration of the relationship between technology and Nature and its impact on Nature. Here we be are thinking about not only humans, but micro- and macroogranisms, and the rights of Nature. (The granting of forms of legal personhood and human rights for the protection of rivers in New Zealand and Ecuador are illuminating examples).[63] This approach aims to assess the interactions amongst and between components of all Earth systems: the lithosphere, atmosphere, hydrosphere and biosphere. The FLE^{5}SH framework provides a common toolbox that diverse stakeholders – researchers, policymakers, regional and national social movements, civil society organisations, and others – can use to evaluate technologies and if warranted, to choose a different future.

At present, many products and services are coming to market without pre-market review and without comprehensive impact assessments. Regulators have generally held back and there is a general tendency to let the market decide and promote industry self-regulation. The law may have a history of struggling to keep up with technological progress, but we should not accept this as a permanent state of affairs that stops discussion of appropriate regulation and accountability. Unforeseen harms can occur if there is no incentive for a company to behave responsibly other than loss of reputation. Fines for violating laws may be regarded as a cost of doing business.

In relation to discussion of technology assessment, we suggest utilizing the Precautionary Principle. This principle has been invoked in the context of environmental policy, as well as in the context of public health. It is an important principle in International Environmental Law and is set out in the Rio Declaration on Environment and Development (1992). Principle 15 of the Rio Declaration:

> 'In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation.'[64]

It is also set out in article 191 of the Treaty on the Functioning of the European Union.[65]

A useful depiction of when the Precautionary Principle ought to be relied upon stems from the Consensus Statement on the Precautionary Principle developed by the Wingspread Conference on the Precautionary Principle held in 1998 provides that:

> 'When an activity raises threats of harm to human health or the environment, precautionary measures should be taken even if some cause and effect relationships are not fully established scientifically. In this context the proponent of an activity, rather than the public, should bear the burden of proof.'[66]

The Consensus Statement further suggests that:

> 'The process of applying the Precautionary Principle must be open, informed and democratic and must include potentially affected parties. It must also involve an examination of the full range of alternatives, including no action.'[67]

Once the Principle is triggered in relation to a particular technology, when more scientific information becomes available that would enable for assessment, the situation should then be reviewed.[68]

While the Precautionary Principle has often been invoked in the context of environmental protection, as Som *et al* suggest, it can also be applied to social subjects and in thinking about potential frameworks for an information society that is sustainable.[69] We suggest the need for invoking this Principle in the context of consideration of whether to adopt these new technologies. Although smart infrastructure has been promoted as facilitating the development of more sustainable, cost effective, and efficient cities, connecting things such as energy, water and monetary supply chains to the Internet renders them vulnerable to physical and cyber attacks.[70]

4 Conclusion

It is hoped that this paper will stimulate reflection about the following matters: the need to engage in a more public, democratic, and open discussion of technologies and their potential impact on society, the environment, and the planet; the need for greater oversight of technologies that pose significant risks to human or environmental health; the need to ensure that technologies that allow for the alteration of the genetic makeup of biological organisms are subject to oversight, especially regarding their safety; and the need for the development of appropriate laws and governance mechanisms that will protect the public, the environment, and the planet as a whole.

It should be noted that we have developed bodies of law such as consumer protection and product liability law for sound reasons. Permitting commercialization of technologies without any regulation other than industry-self regulation is unlikely to lead to a safer, fairer world. The issues raised both by developments in AI which could lead to a super intelligent AI and others that could lead to the merging of humans with machines raise issues that need to be considered from a range of perspectives. If the future is humanity 2.0 then this should be a choice that humans make, just as if super intelligent AI is to develop, we do need to ensure that its values are in line with those of humanity and the planet. However, there is a pluriversal and not just a universal notion of what constitutes value.[71] Perhaps, a more holistic approach to assessing technology could also serve to guide policy contextually, as a substitute for humanity's conscience, and thereby shape technology in a consistent and more balanced way.

Acknowledgements

Thanks to our colleagues for their support and fruitful discussion on these topics.

References

[1] Shakespeare, W. (reprint, 1st ed 1609) Sonnet 141. In B. A. Mowat & P Werstine (Eds.), Shakespeare's Sonnets (reissue 2004) New York, USA: Simon & Schuster.

[2] Phillips, A.M., Mian, I.S. & Charbonneau, J. 2015, Molecule say 'hello' to molecule: Technological Innovation under the Microscope. In GikII Conference Berlin (http://www.gikii.org/?p=280) ;see also Andelka M. Phillips. 2016. Wake Up and Smell the Coffee! A FLE[5]SH approach to new and emerging technologies … beyond 'Responsible Research and Innovation. University of Edinburgh's IP/IT/Media Law Discussion Group seminar (Edinburgh Law Faculty, 8th February 2016) (http://www.iash.ed.ac.uk/news-and-events/event/andelka-phillips-wake-up-and-smell-the-coffee-a-fle5sh-approach-to-new-and-emerging-technologies-beyond-responsible-research-and-innovation/)

[3] Kearns, T. B. (1998). Technology and the right to privacy: the convergence of surveillance and information privacy concerns. Wm. & Mary Bill Rts. J., 7, 975; O'Brolcháin, F., Jacquemard, T., Monaghan, D., O'Connor, N., Novitzky, P., & Gordijn, B. (2016). The convergence of virtual reality and social networks: threats to privacy and autonomy. Science and Engineering Ethics. 22(1), 1-29; Perakslis, C., Michael, K., & Michael, M. G. (2016). Smart Environments & The Convergence of the Veillances: Privacy Violations to Consider. MBA Faculty Conference Papers & Journal Articles. Paper 92. http://scholarsarchive.jwu.edu/mba_fac/92

[4] Weber, R. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26, 23-30. Internet of Things – New security and privacy challenges doi: https://doi.org/10.1016/j.clsr.2009.11.008; European Commission. (2013) Report on the public consultation on IoT governance. https://ec.europa.eu/digital-single-market/en/news/conclusions-internet-things-public-consultation ; Global Privacy Enforcement Network. (2016). GPEN Privacy Sweep, Internet of Things: Participating Authorities' Press Releases. Retrieved from https://www.privacyenforcement.net/node/717; UK Information Commissioner's Office. (2016, Sep. 22). Privacy regulators study finds Internet of Things shortfalls. Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/privacy-regulators-study-finds-internet-of-things-shortfalls/

[5] Frey, C.B., & Osborne, M. et al. (2016, Jan.). Technology at Work v2.0: The Future Is Not What It Used to Be. Oxford Martin School and CITI GPS Reports. Retrieved from http://www.oxfordmartin.ox.ac.uk/publications/view/2092 ; Williams, L. (2017, Aug. 28). Driverless lorries could mean 600,000 lost jobs. It's time we took a universal basic income seriously. Evolve Politics. Retrieved from http://evolvepolitics.com/driverless-lorries-could-mean-600000-lost-jobs-its-time-we-took-a-universal-basic-income-seriously/ ; Solon, O. (2016, Jun. 17). Self-driving trucks: what's the future for America's 3.5 million truckers? The Guardian. Retrieved from https://www.theguardian.com/technology/2016/jun/17/self-driving-trucks-impact-on-drivers-jobs-us

[6] Simonite, T. (2017, June 23). Google Unveils An AI Investment Fund. It's Betting On An App Store For Algorithms. Wired https://www.wired.com/story/google-ai-venture-fund/ ; Peet, A., & Wilde, T. (2017, Feb). Artificial Intelligence: The Investment Of 2017 And Beyond' Financier Worldwide https://www.financierworldwide.com/artificial-intelligence-the-investment-of-2017-and-beyond/ ; Patterson, A. (2017, July 11). Introducing Gradient Ventures. Google Blog https://www.blog.google/topics/machine-learning/introducing-gradient-ventures/

[7] Neurable, (2017) Retrieved from http://www.neurable.com 25 August 2017.

[8] Dormehl, L. (2017, Aug. 25). Engineers Just Created A Tiny Antenna, Which Could Be Used For Brain Implants. Digital Trends. Retrieved from https://www.digitaltrends.com/cool-tech/tiny-antenna-brain-implant/ 25 August 2017; Nan, T., et al. (2017, Aug. 22) Acoustically actuated ultra-compact NEMS magnetoelectric antennas. Nat Commun, 8(1), 296. doi: 10.1038/s41467-017-00343-8.

[9] Constine, K. (2017, Aug. 25). Elon Musk's brain interface startup Neuralink files $27M fundraise. TechCrunch. Retrieved from https://techcrunch.com/2017/08/25/elon-musks-brain-interface-startup-neuralink-files-27m-fundraise/ 25 August 2017.

[10] See for instance, Barfield, W. (2015) Cyber-Humans: Our Future with Machines (pp. 1-20). Copernicus Books, Springer.

[11] See for example Barfield, W. (2015) Cyber-Humans: Our Future with Machines (pp.1-2). Copernicus Books, Springer.

[12] See note 2 above. This paper builds upon and extends work presented first in 2015 and subsequently in 2016. We are currently working on a number of related papers, and the current paper is based on material in a manuscript to be posted on arXiv later this year, which we also hope to publish in a journal within the next year. This older paper is a survey of the ways in which people and places are under dynamic surveillance and suggests that living in a Panopticon City is akin to being part of a Biological-Behavioural-Geographic-Economic-Social-Physical-Medical Complex.

[13] Please refer to the related paper in this conference: Chang, M., Huang, C.-H., & I.S. Mian, (2017, Sep. 6-7) Economic policy, 'alternative data' and global agriculture: from the trans-Atlantic slave trade to agroecology. In Data For Policy Government by Algorithm? London.

[14] Neurable, retrieved from http://www.neurable.com 25 August 2017; Neurable, (2016, Dec.). Neurable Funded to Power Brain-Controlled Virtual Reality. Press Release retrieved from http://www.neurable.com/news/neurable-funded-power-brain-controlled-virtual-reality 25 August 2017; Metz, R. (2017, Mar.). Controlling VR with Your Mind. MIT Tech Review http://www.neurable.com/news/controlling-vr-your-mind 25 August 2017; and Neurovigil http://neurovigil.com/index.php/technology/ibrain-device 25 August 2017 and Suzuki T., Fujimaki N., & Ichikawa, K. (2007) iBrain: a simulation and visualization tool for activation of brain areas on a realistic 3D brain image. BMC Neuroscience, 8(Suppl 2)P13. doi:10.1186/1471-2202-8-S2-P13.

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4436429/pdf/1471-2202-8-S2-P13.pdf

[15] Berkeley Robotics & Human Engineering Laboratory BLEEX, retrieved from http://bleex.me.berkeley.edu/research/exoskeleton/bleex/ 25 August 2017; and Berkeley Robotics & Human Engineering Laboratory Human Universal Load Carrier (HULC), retrieved from http://bleex.me.berkeley.edu/research/exoskeleton/hulc/ 25 August 2017.

[16] Neuralink, retrieved from https://www.neuralink.com 25 August 2017; Statt, N. (2017, Mar. 27). Elon Musk launches Neuralink, a venture to merge the human brain with AI. The Verge. Retrieved from https://www.theverge.com/2017/3/27/15077864/elon-musk-neuralink-brain-computer-interface-ai-cyborgs; Hull, D. (2017, Aug. 25). Elon Musk's Neuralink Gets $27 Million to Build Brain Computers. Bloomberg Technology. Retrieved from https://www.bloomberg.com/news/articles/2017-08-25/elon-musk-s-neuralink-gets-27-million-to-build-brain-computers

[17] Trafton, A. (2016, Oct. 30). Nanobionic spinach plants can detect explosives. MIT News. Retrieved from http://news.mit.edu/2016/nanobionic-spinach-plants-detect-explosives-1031

[18] Gao, W., Dong, R., Thamphiwatana, S., Li, J., Gao, W., Zhang, L. & Wang, J. (2015). Artificial micromotors in the mouse's stomach: A step toward in vivo use of synthetic motors. ACS Nano 9(1) 117-123. Retrieved from http://pubs.acs.org/doi/ipdf/10.1021/nn507097k ; Seppala, T. J., (2015, Jan. 23). Scientists successfully implant self-destructing nanobots into live mice. Engadget. Retrieved from https://www.engadget.com/2015/01/23/nanobots-in-mice-do-the-twist/

[19] Young, S.L. (2017). Unintended consequences of 21st Century technology for agricultural pest management. EMBO reports (2017) e201744660. doi: 10.15252/embr.201744660. Published online 07.08.2017; Ma, Hong, et al. (2017). Correction of a pathogenic gene mutation in human embryos. Nature. 548(7668), 413-419; Sanders, R. (July 2017, Jul. 19). Defense department pours $65 million into making CRISPR safer. Berkeley News. Retrieved from http://news.berkeley.edu/2017/07/19/defense-department-pours-65-million-into-making-crispr-safer/

[20] Tuptuk, N., & Hailes, S. (2016, Jan. 13). The cyberattack on Ukraine's power grid is a warning of what's to come. The Conversation. Retrieved from http://theconversation.com/the-cyberattack-on-ukraines-power-grid-is-a-warning-of-whats-to-come-52832; Hahn, A., Ashok, A., Sridhar, S. and Govindarasu, M. (2013). Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. IEEE Transactions on Smart Grid. 4(2), 847-855; Mo, Y., Kim, T.H.J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber–physical security of a smart grid infrastructure. Proceedings of the IEEE. 100(1), 195-209.

[21] O'Connell, M. (2017). To Be A Machine (pp. 55-6). London: Granta Publications.

[22] Phillips, A. M. (2017). Reading the fine print when buying your genetic self online: direct-to-consumer genetic testing terms and conditions. New Genetics and Society. 36(3), 273-295, 285 citing *Montgomery (Appellant) v Lanarkshire Health Board (Respondent) (Scotland)* [2015] 2 All ER 1031, [2015] UKSC 11 and Campbell, M. (2015). Montgomery v Lanarkshire Health Board. Common Law World Review 44(3), 222–228.

[23] Coffey, H. 'The future is here – a Swedish rail company is trialling letting passengers use biometric chips as tickets' The Independent (16 June 2017) http://www.independent.co.uk/travel/news-and-advice/sj-rail-train-tickets-hand-implant-microchip-biometric-sweden-a7793641.html

[24] Brooks, J. 'A Swedish start-up has started implanting microchips into its employees' CNBC (3 April 2017) https://www.cnbc.com/2017/04/03/start-up-epicenter-implants-employees-with-microchips.html ; Grimm, N. 'Swedish employees agree to free microchip implants designed for office work' ABC News (3 April 2017) http://www.abc.net.au/news/2017-04-03/swedish-employees-agree-to-microchip-implants/8410018 ; Michael, K., Aloudat, A., Michael, M.G., & Perakslis, C. (2017).You Want to Do What with RFID?: Perceptions of radio-frequency identification implants for employee identification in the workplace. IEEE Consumer Electronics Magazine. 6(3), 111-117; (2017, Apr. 4) Swedish company Epicenter implants microchips into employees' News.com.au. Retrieved from http://www.news.com.au/technology/science/human-body/swedish-company-epicenter-implants-microchips-into-employees/news-story/5c48700ebb54262ae389db085593ab12; Sheppard, D. (2017, Aug. 22). Microchipping workers: What are the moral, practical and legal implications? Personnel Today. Retrieved from http://www.personneltoday.com/hr/microchipping-workers-moral-practical-legal-implications/ ; Solon, O. (2017, Aug. 2).World's lamest cyborg? My microchip isn't cool now – but it could be the future. The Guardian. https://www.theguardian.com/technology/2017/aug/02/microchip-contactless-payment-three-square-market-biohax ; Associated Press. (2017, Apr. 3). Companies start implanting microchips into workers' bodies. LA Times. Retrieved from http://www.latimes.com/business/technology/la-fi-tn-microchip-employees-20170403-story.html

[25] Constine, J. (2017, Apr. 19). Facebook is building brain-computer interfaces for typing and skin-hearing. TechCrunch. Retrieved from https://techcrunch.com/2017/04/19/facebook-brain-interface/ ; Strickland, E. (2017, Apr. 20). Facebook Announces 'Typing-by-Brain' Project. IEEE Spectrum Retrieved from http://spectrum.ieee.org/the-human-

os/biomedical/bionics/facebook-announces-typing-by-brain-project

[26] Sørensen, E. J.B. (2016). The post that wasn't: Facebook monitors everything users type and not publish. Computer Law & Security Review, 32(1), 146-151.

[27] Duhigg, C. (2012, Feb. 16). How Companies Learn Your Secrets. New York Times Magazine. Retrieved from http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1&hp=&pagewanted=all ; Lubin, G. (2012, Feb. 16). The Incredible Story Of How Target Exposed A Teen Girl's Pregnancy. Business Insider. Retrieved from http://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2?IR=T ; Papadopoulos, Elias P., et al. 'The Long-Standing Privacy Debate: Mobile Websites Vs Mobile Apps.' *Proceedings of the 26th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 2017; Narayanan, Arvind, and Dillon Reisman. 'The Princeton Web Transparency and Accountability Project.' *Transparent Data Mining for Big and Small Data*. Springer International Publishing, 2017. 45-67.

[28] Ellenberg, J. 'What's Even Creepier Than Target Guessing That You're Pregnant?' Slate (19 June 2014) http://www.slate.com/articles/life/dear_prudence/2017/08/dear_prudence_my_girlfriend_won_t_donate_to_harvey_victims_because_some.html

[29] Li, Q., Ding, D., & Conti, M. (2015). Brain-computer interface applications: Security and privacy challenges. Communications and Network Security (CNS). In IEEE Conference on ((pp. 663-666). IEEE; Bonaci, T., Calo, R., & Chizeck, H. J. (2014). App stores for the brain: Privacy & security in Brain-Computer Interfaces. In Ethics in Science, Technology and Engineering, 2014 IEEE International Symposium on (pp. 1-7). IEEE.

[30] Ney, P., Koscher, K., Organick, L., Ceze, L., & Kohno, T. (2017). Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More. In USENIX Security Symposium; addition information at https://dnasec.cs.washington.edu/. Retreived from http://dnasec.cs.washington.edu/dnasec.pdf ; Tracy, P. (2017, Aug. 10). Infected DNA successfully hacks computer in terrifying experiment. The Daily Dot. Retrieved from https://www.dailydot.com/debug/dna-hack-computer/; Greenberg, A. (2017, Aug. 10). Biohackers Encoded Malware In A Strand Of DNA. Wired. Retrieved from https://www.wired.com/story/malware-dna-hack; Timmer, J. (2017, Aug. 12). Researchers encode malware in DNA, compromise DNA sequencing software. Ars Technica. Retrieved from https://arstechnica.com/science/2017/08/researchers-encode-malware-in-dna-compromise-dna-sequencing-software/

[31] Calo, R., Froomkin, A.M., and Kerr, I. (2016). Robot Law (pp. 1-22). MA: Edward Elgar Publishing; Walter, D. (2016, Mar. 18). When AI rules the world: what SF novels tell us about our future overlords. The Guardian https://www.theguardian.com/books/booksblog/2016/mar/18/ai-sf-novels-artificial-intelligence-science-fiction-gibson-neuromancer ; Warwick, K. (2016, Nov. 10). The Future of Artificial Intelligence and Cybernetics. MIT Technology Review. Retrieved from https://www.technologyreview.com/s/602830/the-future-of-artificial-intelligence-and-cybernetics/

[32] Committee on Legal Affairs/ (2016, 31 May). Draft Report with recommendations to the Commission on Civil Law Rules on Robotics. Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE582.443

[33] See note 2.

[34] ETC Group. (2017, May). The Wisdom of G.O.A.T.S. (Global Overview Assessment of Technological Systems). Draft Proposal for STI Forum 2, New York. Retrieved from http://www.etcgroup.org/sites/www.etcgroup.org/files/files/etc_goats_us_may2017.pdf ; UN Sustainable Development Knowledge Platform https://sustainabledevelopment.un.org/tfm

[35] ETC Group. (2017, May). The Wisdom of G.O.A.T.S. (Global Overview Assessment of Technological Systems) (p.1). Draft Proposal for STI Forum 2, New York. Retrieved from http://www.etcgroup.org/sites/www.etcgroup.org/files/files/etc_goats_us_may2017.pdf

[36] ETC Group. (2017, May). The Wisdom of G.O.A.T.S. (Global Overview Assessment of Technological Systems). (pp.1-2). Draft Proposal for STI Forum 2, New York. Retrieved from http://www.etcgroup.org/sites/www.etcgroup.org/files/files/etc_goats_us_may2017.pdf

[37] ETC Group. (2017, May). The Wisdom of G.O.A.T.S. (Global Overview Assessment of Technological Systems). (pp.1-2). Draft Proposal for STI Forum 2, New York. Retrieved from http://www.etcgroup.org/sites/www.etcgroup.org/files/files/etc_goats_us_may2017.pdf

[38] Mi Pulse. Retrieved from https://www.mi-pulse.com accessed 29 August 2017; Vitali. Retrieved from https://vitaliwear.com

[39] Chauriye, N. (2016). Wearable Devices as Admissible Evidence: Technology is Killing Our Opportunity to Lie. 24(2) Catholic University Journal of Law and Technology. 24(2)(9), 494-528. Retrieved from http://scholarship.law.edu/cgi/viewcontent.cgi?article=1018&context=jlt&sei-redir=1&referer=https%3A%2F%2Fscholar.google.co.uk%2Fscholar%3Fq%3Dfitbit%2Bused%2Bas%2Bevidence%2Bsexual%2Bassault%2Bflorida%26btnG%3D%26hl%3Den%26as_sdt%3D0%252C5#search=%22fitbit%20used%20as%20evidence%20sexual%20assault%20florida%22%20 ; Jackson, B. A., Banks, D., Woods, D., & Dawson, J.C. (2017). Future-Proofing Justice: Building a Research Agenda to Address the Effects of Technological Change on the Protection of Constitutional Rights. Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR1748.html.

[40] Irish Data Protection Commissioner. (2016, Sep. 22). Findings of International Privacy Sweep 2016 published. Retrieved from https://www.dataprotection.ie/docs/23-9-2016-International-Privacy-Sweep-2016/i/1597.htm ; Privacy Commissioner (New Zealand). (2016, Sep. 28). International study finds privacy shortfalls in Internet of Things devices. Retrieved from https://www.privacy.org.nz/news-and-publications/statements-media-releases/international-study-finds-privacy-shortfalls-in-internet-of-things-devices/ ; and UK Information Commissioner's Office. (2016, Sep. 22). Privacy regulators study finds Internet of Things shortfalls. Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/privacy-regulators-study-finds-internet-of-things-shortfalls/

[41] Hilts, A., Parson, C., & Knockel, J. (2016). Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security (pp24, 31-33). Open Effect Report. Retrieved from https://openeffect.ca/reports/Every_Step_You_Fake.pdf ;HPE

Fortify and the Internet of Things. (2015). Internet of Things Security Study: Smartwatches. Retrieved from http://go.saas.hpe.com/fod/internet-of-things ; see also HP. (2015, Jul. 22). HP Study Reveals Smartwatches Vulnerable to Attack. HP News Advisory. Retrieved from http://www8.hp.com/us/en/hp-news/press-release.html?id=2037386

[42] Drabiak, K. (2017). Caveat Emptor: How the Intersection of Big Data and Consumer Genomics Exponentially Increases Informational Privacy Risks. Health Matrix, 27, 143-525;

[43] Nick Bostrom. (2014). Superintelligence: Paths, dangers, strategies (pp.4, and 62-77). Oxford: Oxford University Press.

[44] Nick Bostrom. (2014). Superintelligence: Paths, dangers, strategies (pp. 22-23). Oxford: Oxford University Press.

[45] Nick Bostrom. (2014). Superintelligence: Paths, dangers, strategies (pp. 260-1). Oxford: Oxford University Press.

[46] Vincent, J. (2017, Aug. 21). Elon Musk and AI leaders call for a ban on killer robots. The Verge. Retrieved from https://www.theverge.com/2017/8/21/16177828/killer-robots-ban-elon-musk-un-petition ;Future of Life Institute. (2017). Autonomous Weapons: An Open Letter From AI & Robotics Researchers. Retrieved from https://futureoflife.org/open-letter-autonomous-weapons/ ; Future of Life Institute, (2017, Aug. 20). Killer robots: World's top AI and robotics companies urge United Nations to ban lethal autonomous weapons. Retrieved from https://futureoflife.org/2017/08/20/killer-robots-worlds-top-ai-robotics-companies-urge-united-nations-ban-lethal-autonomous-weapons/

[47] Burgess, M. (2017, Feb. 9). DeepMind's AI has learnt to become 'highly aggressive' when it feels like it's going to lose. Wired. Retrieved from http://www.wired.co.uk/article/artificial-intelligence-social-impact-deepmind; Leibo J.Z., Zambaldi, V., Lanctot, M., Marecki, J., &Graepel T. (2017, May). Multi-agent Reinforcement Learning in Sequential Social Dilemmas. In Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems (pp. 464-473). International Foundation for Autonomous Agents and Multiagent Systems. Retrieved from https://storage.googleapis.com/deepmind-media/papers/multi-agent-rl-in-ssd.pdf

[48] Etzioni, A., & Etzioni, O. (2016). Designing AI systems that obey our laws and values. Communications of the ACM 59(9) 29-31. Retrieved from https://pdfs.semanticscholar.org/260f/4a655a63e9f0e8867140a8797e7a64e0cdd2.pdf ; Bonnefon, J. F., Shariff, A., & Rahwan, I. (2015). Autonomous vehicles need experimental ethics: are we ready for utilitarian cars?. arXiv preprint arXiv:1510.03346. Retrieved from https://pdfs.semanticscholar.org/13d4/56d4c53d7b03b90ba59845a8f61b23b9f6e8.pdf ; Bradshaw-Martin, H., & Easton, C. (2014). Autonomous or 'driverless' cars and disability: a legal and ethical analysis. European Journal of Current Legal Issues, 20(3). Retrieved from http://webjcli.org/article/view/344/471

[49]Mignolo, W. (2013, Oct. 20). On Pluriversality. Retrieved from http://waltermignolo.com/on-pluriversality/ Mignolo, W. (2010) The communal and the decolonial. Turbulence. Retrieved from http://www.turbulence.org.uk/index.html@p=391.html ; Grosfoguel, R., (2012). Decolonizing Western uni-versalisms: decolonial pluri-versalism from Aimé Césaire to the zapatistas. Transmodernity: Journal of Peripheral Cultural Production of the Luso-Hispanic World, 1(3), 88-104. Retrieved from http://escholarship.org/uc/item/01w7163v

[50] Clarke, A. C., (1st ed. 1968, 2016). 2001: A Space Odyssey. (Reprint). Penguin Books.

[51] Bradley-Munn, S.R., & Katina, M. (2016). Whose Body Is It?: The body as physical capital in a techno-society. IEEE Consumer Electronics Magazine 5(3), 107-114; Barfield, W. (2015) Cyber-Humans: Our Future with Machines (pp. 135-176). Copernicus Books, Springer.; Mallonee, L. (2017, Jun. 8). The DIY Cyborgs Hacking Their Bodies For Fun. Wired. Retrieved from https://www.wired.com/story/hannes-wiedemann-grinders/

[52] Constine, J. (2017, Jun. 27). Facebook now has 2 billion monthly users… and responsibility. TechCrunch. Retrieved from https://techcrunch.com/2017/06/27/facebook-2-billion-users/

[53] Morris, I. (2017, Jun. 29). Apple Has Sold 1.2 Billion iPhones Worth $738 Billion In 10 Years. Forbes. Retrieved from https://www.forbes.com/sites/ianmorris/2017/06/29/apple-has-sold-1-2-billion-iphones-worth-738-billion-in-10-years/

[54] Statistica, (2017). Number of smartphone users worldwide from 2014 to 2020 (in billions). Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[55] Vince, G. (2012, Nov. 29). The high cost of our throwaway culture. BBC. Retrieved from http://www.bbc.com/future/story/20121129-the-cost-of-our-throwaway-culture

[56] Starritt, A. (2016, Oct. 27). Sweden is paying people to fix their belongings instead of throwing them away. World Economic Forum. Retrieved from https://www.weforum.org/agenda/2016/10/sweden-is-tackling-its-throwaway-culture-with-tax-breaks-on-repairs-will-it-work/

[57] Federal Trade Commission. (2017, Jan.) Cross-Device Tracking. Staff Report. Retrieved from https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf ; Brookman, J., Rouge, P., Alva, A., & Yeung, C., (2017). Cross-Device Tracking: Measurement and Disclosures. In Proceedings on Privacy Enhancing Technologies 2017(2),133-148; Chen, K., Wang, X., Chen, Y., Wang, P., Lee, Y., Wang, X., Ma, B., Wang, A., Zhang, Y. & Zou, W. (2016). Following devil's footprints: Cross-Platform Analysis of Potentially Harmful Libraries On Android and iOS. In Security and Privacy (SP), 2016 IEEE Symposium on (pp. 357-76). IEEE. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7546512

[58] General Data Protection Regulation 2016/679. European Union; 2016. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

[59] See note 2.

[60] Please refer to the related paper in this conference: Chang, M., Huang, C.-H., & I.S. Mian, (2017, Sep. 6-7) Economic policy, 'alternative data' and global agriculture: from the trans-Atlantic slave trade to agroecology. In Data For Policy Government by Algorithm? London.

[61] ETC Group. (2011, Mar.). Why Technology Assessment? ETC Group Briefing Paper: New York. Retrieved from http://www.etcgroup.org/sites/www.etcgroup.org/files/Why%20technology%20assessment2011.pdf ; (2015, Jul. 16). UN moves towards a technology early listening system. ETC Group, News Release. Retrieved from http://www.etcgroup.org/content/un-moves-towards-technology-early-listening-system. ; Daño, N.,

Wetter, K. J., & Ribeiro, S. (2013, Dec. 9-13). Addressing the 'Technology Divides': Critical Issues in Technology and SDGs. Briefing Paper: Science, Technology and Innovation (STI) 6th Session of the Open Working Group on Sustainable Development Goals: New York. Retrieved from https://sustainabledevelopment.un.org/content/documents/4673dano.pdf. ; Wolbring, G., (2009, Dec. 14). Innovation for whom? Innovation for what? The Impact of Ableism. *2020 Science* Guest Blog. Retrieved from http://2020science.org/2009/12/14/wolbring/. ; ETC Group, (2014, May 29). A Note for Discussion: UN Technology Assessment. Retrieved from http://www.un-ngls.org/IMG/pdf/Technology_Assessment_Overview21May2014.pdf.

[62] Reijers, W., O'Brolcháin, F., & Haynes, P. (2016). Governance in Blockchain Technologies & Social Contract Theories. Ledger, 1, 134-151. Doi: 10.5915/LEDGER.2016.62

[63] See for example the recent New Zealand Te Awa Tupua (Whanganui River Claims Settlement) Act 2017. Retrieved from http://www.legislation.govt.nz/act/public/2017/0007/latest/DLM6830851.html ; Tanasescu, M. (2017, Jun. 19). Rivers Get Human Rights: They Can Sue to Protect Themselves. Scientific American. Retrieved from https://www.scientificamerican.com/article/rivers-get-human-rights-they-can-sue-to-protect-themselves/ ; O'Donnell, E., & Talbot-James, J. (2017, Mar. 23). Three rivers are now legally people – but that's just the start of looking after them. The Conversation. Retrieved from https://theconversation.com/three-rivers-are-now-legally-people-but-thats-just-the-start-of-looking-after-them-74983?sr=3 ; Biggs, S. (2017, Apr. 17). When Rivers Hold Legal Rights. Earth Island Journal. Retrieved from http://www.earthisland.org/journal/index.php/elist/eListRead/when_rivers_hold_legal_rights/ ;Community Environmental Legal Defense Fund (2015, Aug. 4, updated 2017, May 19). Rights of Nature: Overview. Retrieved from https://celdf.org/rights/rights-of-nature/ ;Global Alliance for the Rights of Nature. Retrieved from http://therightsofnature.org

[64] Rio Declaration on Environment and Development. (1992) principle 15. Retrieved from http://www.unesco.org/education/pdf/RIO_E.PDF

[65] Treaty on the Functioning of the European Union (2007). Official Journal C 326 , 26/10/2012 P. 0001 – 0390. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

[66] Science and Environmental Health Network. (1998). The Wingspread Consensus Statement on the Precautionary Principle. Retrieved from http://sehn.org/wingspread-conference-on-the-precautionary-principle/ ; See also Kriebel, D., Tickner, J., Epstein, P., Lemons, J., Levins, R., Loechler, E. L., & Stoto, M. (2001). The precautionary principle in environmental science. Environmental Health Perspectives. 109(9), 871–876, 871, citing Raffensperger, C., & Tickner, J. A. (Eds.). (1999). Protecting public health and the environment: implementing the precautionary principle (p.8). Island Press.

[67] Science and Environmental Health Network. (1998). The Wingspread Consensus Statement on the Precautionary Principle. Retrieved from http://sehn.org/wingspread-conference-on-the-precautionary-principle/

[68] Som, C., Hilty, L. M., & Kohler, A. R., (2009). The Precautionary Principle as a Framework for a Sustainable Information Society. Journal of Business Ethics 85, 493. doi: 10.1007/s10551-009-0214-x Communication from the Commission on the precautionary principle /* COM/2000/0001 final */Precautionary Principle. EUR-Lex, Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52000DC0001

[69] Som, C., Hilty, L. M., & Kohler, A. R., (2009). The Precautionary Principle as a Framework for a Sustainable Information Society. Journal of Business Ethics 85, 493. doi: 10.1007/s10551-009-0214-x; Danaher, J. (2016, Mar. 15). New Technologies as Social Experiments: An Ethical Framework. Philosophical Disquisitions. Retrieved from http://philosophicaldisquisitions.blogspot.co.uk/2016/03/new-technologies-as-social-experiments.html.

[70] Taylor, H. (2015, Dec. 28). Biggest cybersecurity threats in 2016. CNBC. Retrieved from http://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html.

[71] Mignolo, W. (2013, Oct. 20). On Pluriversality. Retrieved from http://waltermignolo.com/on-pluriversality/ Mignolo, W. (2010) The communal and the decolonial. Turbulence. Retrieved from http://www.turbulence.org.uk/index.html@p=391.html ; Grosfoguel, R., (2012). Decolonizing Western uni-versalisms: decolonial pluri-versalism from Aimé Césaire to the zapatistas. Transmodernity: Journal of Peripheral Cultural Production of the Luso-Hispanic World, 1(3), 88-104. Retrieved from http://escholarship.org/uc/item/01w7163v