Artificial Jurisprudence: Understanding the Consequences of Emerging Technologies for Human Rights and the Role of Technology Activism

MHR Professional Paper

In Partial Fulfillment of the Master of Human Rights Degree Requirements
The Hubert H. Humphrey Institute of Public Affairs
The University of Minnesota

J.T. Davies
May 6, 2022

Professor Joachim Savelsberg — Date of Oral Presentation
Signature of Paper Supervisor, certifying succssful completion of oral presentation

Professor Jeffrey Yost — Date of Oral Presentation
Signature of First Committee Member, certifying succssful completion of oral presentation

1 Acronyms and Terminology

CJEU - Court of Justice of the European Union

EU - European Union

ECtHR - European Court of Human Rights

FOSS - Free and open source software

GDPR - General Data Protection Regulation (EU law)

NIST - National Institute of Science and Technology (US federal government agency)

2 Introduction

Information technology and computer networks have the potential to catalyse some of the greatest social transformation in history. However, the rapid development of these technologies stands to outpace policy governing them - especially in the arena of human rights. While information technology has the potential to solve numerous problems, such as coordinating vast logistics systems to reduce food waste; or automating simple home functions to improve quality of life for the disabled, it also provides avenues for surveillance, coercion, and control through both state and priva many of which would have been unimaginable when the human rights movement first crystallised.

Some of these technologies, such as blockchain record keeping, have the potential to be used to further the public good; others, such as high-end spyware built with the singular purpose of selling personal data to the highest bidder, have less cause for optimism. These technologies are controlled by a spectrum of actors ranging from publically-traded companies to covert government agencies, and is shielded from scrutiny by both ever-broadening exemptions to oversight in the name of national security, and an increasingly legally restrictive and technically sophisticated international intellectual property system that treats software internals as valuable trade secrets.

We begin with a review of four problems emerging in modern information technology. The ability of algorithmic facial recognition to track individuals without their consent is compounded by the

dangers of misidentification, especially due to the lack of transparency with the internal operations of these systems. This is further complicated by the scale of modern mass surveillance, where the data collected by a single system may be innocuous, but private information can be reconstructed by combining multiple sources, which users may consent to individually without understanding the larger potential for data collection – as well as the potential for that data to be taken from the service provider. We move from surveillance to its sister industry, for-profit cyberwarfare – private companies who specialise in breaking into computer systems for money, both from governments and private citizens. Malware from private companies – often based in Western democracies – has been linked to the surveillance of human rights defenders and journalists worldwide by taking advantage of security flaws in digital devices that are increasingly essential for those careers. Finally, we examine the dictum of "code is law", originating in the 1990s to indicate how decisions made in technology development are in of themselves policy decisions, and the related question of when and how human operators should intervene in the functions of a technological system used by others.

From here, we move to discuss the predominant modes of rights-based activism within technology spaces – the free and open source movement and repair movement. These movements, which originated from concerns about the ability of manufacturers or vendors to use their control of distribution and maintenance to coerce or exploit users, are relevant to the human rights field not only for the applications of their principles, but for the lessons we can take from them to address technical issues in a broader social sphere.

I firmly believe that we will be unable to address these issues if technology and policy activists do not stand together. It is my hope that by explaining these issues from my own hybrid perspective, I can help to accomplish that goal.

3 Selected Technologies of Concern

3.1 Algorithmic Facial Recognition

Automated image recognition is touted as the next great step forward in identification. In a 2021 study, the National Institute of Science and Technology (NIST) found that the best-performing

facial recognition algorithms were 99.5% accurate in matching a person to pictures of them stored in a database (Grother et al. 2021). For comparison, a 2015 NIST evaluation of single-finger fingerprint matching found an accuracy of 98.1%[1], while two-finger matching had an accuracy of 99.73%.(Watson et al. 2015) Adoption of facial recognition for these purposes has increased significantly during the COVID-19 pandemic. A 2021 survey conducted by the International Air Transport Association (IATA), an international private association[2] whose members control over 80% of passenger air traffic, found that passengers willing to share biometric data (including facial recognition) to expedite security screenings has risen to 73%, compared to only 46% in 2019 (IATA 2021). The IATA would have a lot to gain from such a system - in a 2018 white paper, "identity as a service" was touted as reducing financial risk to airlines, both in terms of improved verification accuracy as well as the potential of offloading liability to service providers (IATA 2018).

Usage of facial recognition technology is traditionally divided into *verification* and *identification*. For a verification system, a user makes a claim about their identity, and the system simply *verifies* that they are who they claim they are. An identification system by contrast has no such claim: an unknown individual is photographed or recorded, and the system attempts to match them to a known identity. In the popular press, "identification" is often used for both – for example, the IATA's press release claims passengers want "biometric identification", but the system described would be referred to technically as identity verification (IATA 2021). (Indeed, the earlier white paper refers to proposals almost exclusively as "verification", unless they explicitly provide both verification and identification services (IATA 2018).) Despite the weight given to this distinction in many discussions of facial recognition, especially in policy and law enforcement spheres, the distinction is largely irrelevant on a technical level, because the underlying technologies needed to perform verification are essentially the same as those needed for identification, and in many cases the systems used are identical. Activists have criticised the reliance on this distinction as a rhetorical tool without substantive technical foundation, and claim proponents are deflecting from

1. More properly, the NIST study tested false negative rates - i.e., 1.9% of single finger tests failed to match the correct prints given a fixed maximum probability of matching incorrect prints. Unlike the facial recognition figure, no single accuracy figure is given within the text itself, as it was testing performance of fingerprinting very generally rather than fitness for a specific purpose.

2. Historically often called a cartel, due to its influence on international ticket prices

or obfuscating rights concerns raised about identification systems by instead focusing on the more specific case of verification, when most systems capable of the latter can still be used (or abused) for the former (Cyphers, Schwartz, and Sheard 2021).

Verification is an attractive core argument for facial recognition advocates. In many regards it is the ideal technical case - matching between two sets of data which ought to be the same or very similar, and looking for significant differences, is in general easier than attempting to match within larger and more diverse sets of data. Users often provide verification data directly, explicitly for the system's use, and thus tend to follow the system's instructions and give data which is easier to work with; that data is (usually) provided by users directly also avoids the ethical questions about consent which many identification systems face.

The ethical issues with automated identification are far from abstract philosophical arguments. In January of 2019, Robert Williams returned home from work only for Detroit police to pull in behind his car and handcuff him in front of his children. The only evidence for his arrest was an erroneous match between grainy security footage and an outdated driver's license photo (Williams 2021). In Feburary, Nijeer Parks was arrested for a crime committed in a town thirty miles away - linked only by a spurious match between Parks' driver's license and the fake ID used by the actual perpetrator. In Parks' words, "the only thing we have in common is the beard". Due to his past convictions, the automated bail system used in New Jersey kept Parks in jail after his first hearing – until evidence proving he was in a different town at the time emerged, Parks had seriously considered falsely pleading guilty just to reduce the potential sentence (Hill 2020). In June, James Craig, Detroit Police Chief at the time of Williams' arrest, said that "if we were just to use the technology by itself," it would misidentify people 96% of the time – though he stressed that this use would be against department policy. Less than a month later, Detroit police arrested Michael Oliver for larceny due to a facial-recognition match; the evidence in question was a single frame from a cell-phone video of a man who looked nothing like him — "he didn't even have tattoos." While the judge agreed and dismissed the case, Oliver still lost his job after missing work to attend his court dates. In October, the City of Detroit renewed the $220,000 contract with their facial recognition software provider (Stokes 2020).

Of the many commonalities between Williams', Parks', and Oliver's cases, the most significant is that all three men were black. Facial recognition systems have consistently shown poorer performance when evaluating non-white subjects; the NIST noted a "generally large" effect of race and ethnicity on facial recognition performance, with the highest rate of false positives occurring in West and East African people. False positive rates vary across by demographics by as much as two orders of magnitude (that is, false positives are more than a hundred times more likely for the worst-performing demographics than the best) (Grother, Ngan, and Hanaoka 2019). Another vital common thread is that the three men were all clearly exonerated by factors which invalidated the flawed result of the facial recognition system, seomthing that is far from certain in every case. Parks' consideration of a false guilty plea to avoid a longer sentence is hardly unique to his case, especially as many prosecurors prefer to push aggressively for plea deals rather than take a case to court.

There is a final risk to facial recognition software. Even if a hypothetical large-scale identification system is deployed which perfectly respects individual rights, the data it uses to function still must be stored and accessed digitally. This data can then be obtained by a third party and connected to other data, without the knowledge of the data subject (or, in the most extreme cases, the service provider). This aggregation of data en masse is already being extensively practiced by governments worldwide, in the name of national security and the so-called war on terror.

3.2 Global Expansion of Mass Surveillance

Interconnected databases allow for the collection of far more data than any individual system would produce. Consider the classical Indian parable of the blind men and the elephant – three blind men encounter an elephant, and try and describe it by touch. One grabs its leg, and says it is a tree; another its trunk, and says it is a snake; the third, its tusk, and says it is a spear. Each of the three men has an individual piece of information which is reasonable from a limited context, but incomplete. This same problem occurs with digital commerce – companies have a vested interest in knowing as much about customer preferences as possible, in order to suggest them products which they are likely to buy, but only have direct access to what a user does with own their services. This

creates a strong incentive to track users across as many services as possible, either by exchanging data between service providers or simply by using a backend service that many other services rely upon. This is what powers the advertising juggernauts of the modern web – with the right algorithm and enough blind men, Google or Facebook's servers reconstruct each individual elephant.

This collection of information, so-called "surveillance capitalism", has attracted opposition from many advocacy groups since the early days of the Internet. This was largely limited to technical circles until the revelation of large-scale involvement by government agencies, particularly in the United States, by Edward Snowden's revelation of the scope of the PRISM program. Building on the infrastructure used to collect personal information for profit, the state would gather all this information to a singular place for any and every user they could reach, regardless of any national security interest. As the data was being collected already, it was easier for the state to simply collect everything, and then sift through it for anything important; what judicial oversight existed, through the classified FISA court, was little more than a rubber stamp.

The FISA court is one of many examples of what I call "judicial lag" – courts, the traditional check on law enforcement and intelligence agencies, often rely on precedent for previous technologies when assessing the impact of new ones, and laws advance far more slowly than technology. A classical example is the United States' Electronic Communications Privacy Act (ECPA) of 1986, which still governs wiretap and search procedures for computer systems today, despite thirty-five years of rapid technological development. The law allows authorities to request personal communications from an Internet service provider without a warrant as long as the communications have been "abandoned" for more than 180 days – "abandoned" in this case meaning it has not been downloaded from the server to the user's computer in that time. In 1986, emails were usually stored on individual user's computers, only being on the service provider's servers until downloaded into the user's inbox; thus, it was rare for an email to remain available to the service provider for more than a day. Most modern email services, by contrast, do not even offer the option to remove emails from the service's systems – meaning that all six-month old emails in the United States can be searched at any time, without any judicial oversight. Though the Court of Appeals for the Sixth Circuit has ruled that it does not apply to cloud services, no federal action has successfully been

taken to modernise the ECPA.

This is not an issue limited to one side of the Atlantic. While the United States only recognises specific restrictions on search and seizure under the Fourth Amendment, the European Court of Human Rights (ECtHR) recognises data protection as a fundamental right. Article 8 of the European Convention on Human Rights, which establishes that "everyone has the right to respect for [their] private and family life, [their] home and [their] correspondence", barring some specific exceptions.[3] However, the ECtHR's stance on data privacy is reversing, in no small part due to the Court's reliance on past cases and outdated technical standards which poorly reflect the capabilities and scope of modern data processing systems. Past rulings on surveillance systems often focused on the narrow use cases of the technology in question, and these rulings are used to justify continued use or expansion of those systems even as the technology becomes ubiquitous in everyday life – quite contrary to the past court's assumptions and intent. Ni Loideain 2020 details the history of ECtHR jurisprudence on surveillance issues, and particularly how it has become less rigourous over time. Despite granting states a widening "margin of appreciation" on matters of national security due to "the increased sophistication of communications technology", the court has consistently failed to update its procedures to properly engage with the realities of 21st-century digital life for citizens.

Ni Loideain 2020 and Christakis and Bouslimani 2019 both cite the *Centrum för Rättvisa v. Sweden* and *Big Brother Watch and others v. the United Kingdom* decisions of 2018 as a significant reversal of ECtHR policy regarding surveillance, stepping back from a "strict necessity" test to instead endorse widespread surveillance as a tool to protect national security. While both of these cases were challenged again before the ECtHR and partly overturned in 2021, many legal experts saw any celebration by privacy activists as short-lived. Rather than recognising bulk surveillance as categorically a human rights issue, the Court only rejected the specific programs for their specific scope, and reinforced the legitimacy of bulk surveillance as a national security tool - in particular, it ruled that accessing stored data was not an interference with Article 8's rights to respect to private life and correspondence, regardless of how that data was obtained (Ni Loideain 2021; Sajfert 2021).

3. "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Surveillance by state actors and law enforcement is often justified as necessary for national security, but the creation of this data poses risks in of itself, even making the unrealistically generous assumption that all information gathered and processed by state actors will be used solely to further the cause of human rights and well-being. The very existence of a database creates an incentive to compromise that data, either to gain access and utilise it, or modify its contents to suit the cracker's own purposes. As states develop these systems, their rivals rush to find vulnerabilities and compromise them; not only rivalries between states, but also non-state actors from militant groups and organised crime to multi-billion-dollar corporations.

3.3 Corporate Cracking

In addition to the challenges of direct state-based surveillance, a lucrative industry of crackers-for-hire[4] has emerged, selling illicit access to data to the highest bidder – or at least the highest acceptable bidder, according to firms' own self-imposed rules on "legitimate" state interest. Where the social contract of cybersecurity is to divulge vulnerabilities to developers or service providers (or to the public if no action is taken), these firms instead keep these exploits as trade secrets to allow them to better break in to targets' devices.

The origins of corporate cracking began in the world of so-called "white hat" hacking. Italian firm HackingTeam was founded in 2003 to provide software audits and penetration testing to clients. Penetration testing — professionals using the same tools and techniques as malicious crackers in order to identify and fix vulnerabilities in systems — is a fundamental pillar of cybersecurity research, and it has historically been one of the major points of contention between efforts to regulate cybercrime and security experts. Many forms of penetration testing are *de jure* illegal under major cybercrime laws, such as the US's Computer Fraud and Abuse Act and Digital Millennium Copyright Act, especially when performed by independent security researchers. Corporate penetration testing firms like the early version of HackingTeam served to bypass this issue, trading some inde-

4. "Cracker" is the preferred term for malicious actors. The popular usage of "hacker" is considered a malappropriation of the cultural hacker identity - individuals who use technical knowledge to push the limits of systems for its own sake, and who then share any knowledge they gain. This cultural sense of hacker is best seen in popular discourse as the root of the term "life hack".

pendence for protection from legal action by the company they are investigating. HackingTeam's corporate fortunes started to rise through a different avenue: instead of performing penetration testing, they found a thriving market in selling their offensive capability first to Italian law enforcement, and then to governments around the world – including documented connections to human rights abuses. As HackingTeam started a billion-dollar industry, CEO David Vincenzetti snidely remarked in an email that they developed "the evilest technology on earth" (Kushner 2016).

HackingTeam faced an ironic turnabout in 2015, when hacktivist and self-proclaimed "anarchist revolutionary" Phineas Fisher (pseud.)[5] extracted 400 gigabytes of data from the company's own network, including the company's complete list of clients and all source code for its tools. Fisher 2016 then released a manifesto-cum-technical breakdown of the HackingTeam attack shortly afterwards, where they identified HackingTeam as allowing oppressive regimes to "spy on journalists, activists, political opposition, and other threats to their power; and, occasionally, on actual criminals and terrorists". While Fisher is open in their own political motivations for the attack, they also charge that firms such as HackingTeam are far from politically neutral themselves. In rejecting the white hat of security research to sell their exploits to governments, Fisher sees them as donning the black shirt of Italian fascism – and not without reason. In the leaked emails, Vincenzetti's messages are often concluded with the phrase "boia chi molla", an Italian Fascist slogan which can be translated as "those who give up are traitors" (Saudelli 2021). The hack and manifesto are dedicated to the victims of the 2001 police raid on the Armando Diaz school, where members of an Italian anti-capitalist group protesting the G8 summit were indiscriminately attacked by police in ski masks, then taken to a detention facility where they were beaten in their cells, sprayed with gas, and forced to sing fascist anthems. Of the over 300 officers who participated in the raid and its aftermath, 15 were convicted - and none of them served prison terms (Davies 2008).

Fisher's attack was the beginning of the end for HackingTeam, and it was bought out by competitor InTheCyber and rebranded as Memento Labs. But HackingTeam's fall has allowed new giants into the playground; more spyware products are on the market than ever before, and as their functionality grows, so does the capacity for abuse.

5. Fisher's pseudonym is derived from FinFisher, another for-profit malware system. Gamma International, FinFisher's developer, was the target of Fisher's first known attack.

The NSO Group, an Israeli technology firm and defense contractor, first developed the program it would label Pegasus in 2011. The software, which can be covertly installed on mobile devices running iOS and Android[6], grants total access to calls, text messages, passwords, applications, and sensors including microphone and camera. The software remained unknown until 2016, when Ahmed Mansoor, a human rights defender operating in the United Arab Emirates, received a text message containing a URL and claims of "new secrets" about human rights violations in Emirati prisons. Suspicious of the link, Mansoor instead forwarded the message to the University of Toronto's Citizen Lab, where researchers discovered it led to a "spear-phishing" attack which would compromise the device and install the Pegasus software when opened – making use of three previously unrevealed vulnerabilities in iOS (Marczak and Scott-Railton 2016). Since the Mansoor revelation, Pegasus has been identified in several countries, often targeting journalists and human rights defenders. Known targets of the program range from the staff of online Salvadoran newspaper *El Faro* (Gavarrete, Reyes, and Martínez 2022), to the ex-wife of the sheikh of Dubai and her lawyers (Holden and Macaskill 2021), to nearly the entire cabinet of French president Emmanuel Macron ("Pegasus Project: Macron among world leaders selected as potential targets of NSO spyware" 2021). NSO Group currently faces a lawsuit over alleged involvement in the murder of Jamal Khashoggi; in a statement to Israeli newspaper Haaretz, an NSO spokesman called the claims "baseless" - not because Pegasus was uninvolved in the Khashoggi case[7], but because the firm is "a technology company that is uninvolved with how our products are used once they are sold to our customers" (Levinson, Harel, and Kubovich 2018). NSO now refuses to respond to media inquiries, calling criticism of the program a "vicious and slanderous campaign" ("Enough is enough! - NSO Group," n.d.) and framing it as politically motivated by anti-Israeli sentiment.ew

Paolo Lezzi, new owner of Memento Labs (HackingTeam), had a simple answer when a journalist asked him how the company would prevent abuse of its tools at a trade event - he pointed to the racks of machine guns at a nearby booth run by an arms manufacturer, and said "Why does no

6. Technically, NSO's Android application is a different program which offers similar functionality; security researchers dubbed the Android variation "Chrysaor", after the brother of the mythological Pegasus. Unless the platform distinction is significant, both are generally referred to collectively as Pegasus in the literature.

7. They claimed there was no evidence of Pegasus's presence, and characterised Citizen Lab's research as "not based in reality", but did not deny selling Pegasus to the Saudi government.

one ask them that question?"[8] (O'Neill 2019)

3.4 "Code is Law": Technology as Policy

The dictum "code is law" was first coined by Harvard law professor Lawrence Lessig to refer to the notion that computer programs regulate behaviour of users independently of legal frameworks built around those systems. Human societies and interactions in meatspace[9] are governed by two kinds of laws - those set by humans, such as speed limits or copyrights, and those imposed by nature, such as the speed of light or the quantum no-cloning theorem. The first set of laws are malleable, and only face social sanctions. There is nothing to *prevent* me from, for instance, driving down the highway at one hundred and twenty miles per hour, with my car full of terabytes of Hollywood films[10]; however, by doing so I would expose myself to consequences determined by society (and likely very expensive). However, even if all the forces of society wished for me to travel down a highway at 700 million miles per hour and fill my car with copies of arbitrary quantum states, there is nothing any of us could do.[11]

Cyberspace, by contrast, shifts the control of "natural laws" to the developers and maintainers of software. While obviously computers must obey the same physical laws as anyone else, these rarely constrain the actions of software users (as long as the system is running properly); instead, users are restricted by what the software allows them to do. I can edit a Wikipedia page because Wikipedia's programming allows it; I can't edit a New York Times article because their progamming doesn't. Arch Linux facilitates near-complete customisation of all but the most fundamental core of the operating system; Microsoft Windows doesn't let me uninstall bundled software that I never use. These are all deliberate decisions made by the developers of the software which impact not only user behaviour with their system, but what they expect from other systems. Some of these, such as Wikipedia's commitment to open editing, are made for ideological reasons; others, such

8. We do, Mr. Lezzi. We do.

9. Physical spaces, antonymous to cyberspace. Lessig uses the term "real space", though by his own admission this is quite a misnomer - digital spaces are as "real" as physical ones for human interaction and society. The term "meatspace" originated as a semi-ironic injoke within hacker culture; it was added to the Oxford English Dictionary in March 2001.

10. There is a classical IT adage that one should never underestimate the bandwidth of a stationwagon full of tape speeding down the freeway.

11. At least, as we presently understand the limitations of the physical universe.

as Microsoft's dogged insistence that I will one day find a use for Edge or Cortana, are more market-driven. In both of these cases, the way the software is written determines what is allowed or forbidden - and not always in ways the developer might intend.

Lessig's axiom was a key part of his argument against the then-common assertion that the Internet was beyond the influence or regulation of government. Lessig's work developed the so-called "pathetic dot theory" of regulation, which sees regulation not as performed by a single actor (the state, or Law), but by four - Law, Market, Norms, and Architecture. The early Internet, in Lessig's view, was an unusual case where Architecture's influence greatly outpaced that of the other regulators - people's behaviours were largely constrained by technology. This has since changed - the centralisation of internet infrastructure under major corporations has seen a sharp rise in market influence on online behaviour, and governments have quickly adopted means to control and surveil online communication. But even now, these forces are subject to the underlying technologies - an issue of particular interest to Lessig is digital restriction management (DRM), which serves to enforce copyright restrictions on digital content. In theory, a copyright only holds for a fixed term and has exemptions for fair use; a DRM scheme, however, does not need to respect these limits.[12] The code, even now, overrides the law.

"Code is law" has taken on another meaning in the world of the blockchain. To cryptocurrency advocates, computerised systems allow for human failings like bias and corruption from system management - instead, a legal system could be built over a system of "smart contracts" consisting of digital computer code which are stored in a decentralised, append-only ledger. The code of these "contracts" serves as a replacement for the broader legal system - a benefit if dealing with high costs of entry, but rigid and inflexible when handling the complex realities of legal contracts. To Lessig, this makes smart contracts "dumb contracts", born in part out of a naive misunderstanding of the relationship between contracts, the state, risk, and the broader legal role of arbitration and ambiguity. While potentially useful for handling very simple interactions (Lessig likens them to a vending machine, where a coin is inserted and soda comes out), these programs can only handle the

12. The COVID-19 pandemic has stressed the importance of public domain exemptions, as many educators struggle to retransmit copyrighted content to students over online streaming platforms due to DRM locking down screen or audio capture on copyright grounds. Copying for educational purposes is explicitly stated by U.S. law to not be a violation of copyright.

(in Lessig's analogy, the off chance that the machine instead dispenses a can of gasoline). Removing the human element from implementation has a further cost - the delicate balance between code maintenance and developer power. Ethereum, the cryptocurrency platform which first adopted a smart contract system, saw this first-hand with the so-called "DAO crisis".

The DAO, which stands for Decentralised Autonomous Organisation, was marketed as a next-generation investment firm, driven by users rather than financiers; using a system of smart contracts, users would deposit their Ethereum tokens into the organisation, which would use it for investment and maintain user balances automatically - allegedly free of human failings, and definitely subject to computational ones. In order to prevent abuse, the contracts that built the DAO were not able to be edited by the developers after the tokens were created without a vote from the DAO's investors. These same contracts contained two programming flaws known as race conditions, essentially allowing users to withdraw tokens multiple times before the system checks if there is tokens in their account to withdraw. Before a vote could be called to address the vulnerability, 3.6 million Ether[13] was extracted from the fund to a private account. In the end, Ethereum's development team stepped in, resetting the blockchain to an earlier state. The community was split - on one hand, investors got their currency back; on the other, flexible human subjectivity had once again overruled the "objective" law of code.[14]

The relationship between code and law can go both ways. Suppose — as in the cases of Robert Williams, Nijeer Parks, and Michael Oliver — that a software system provides the foundation of a criminal prosecution. Under the traditional rights afforded by due process of law, the accused has the right to know the opposing evidence - this is typically taken to be *the output* of a computer program, but the output alone rarely tells the full story.

Consider an extreme example - a hypothetical program which, rather than performing any analysis on an image, simply rolls a die, and reports back a 'match' or 'no match' with an "accuracy" percentage based on the outcome of that roll. If the only thing the program returns in the report are the matching result and the accuracy, this program's output cannot be meaningfully distin-

13. Valued at roughly $50 million USD at the time.

14. The pre-reset Ethereum blockchain, now called "Ethereum Classic", remains active, maintained by users who opposed the reset - largely out of an ideological commitment.

guished from an equally extreme hypothetical program which performs perfect Hollywood-style image reconstruction,[15] but returns the same values.

Of course, there is more accountability than simply taking vendors at their word, including the work done by the NIST – but testing performance does not actually address the question of transparency. *Why* a program reaches a conclusion is just as important as the conclusion it reaches – more important, even, when the issue of discrimination and accountability comes to light. Traditionally, expert evidence such as fingerprinting and laboratory testing consists not only of the results (though they may be what is most relevant to a jury), but also the assurances from the experts performing that work that it was performed according to strongly-defined procedures and held to a specific standard of scientific quality. The internal processes are well-documented, and specific individuals are responsible for following them. In computation, however, the procedures are often trade secrets of the companies providing the software – and it is frequently only those companies' experts who can testify to meeting the company's standards of quality.

The complexity of these systems often means it is difficult to hold either their developers or operators accountable for the outcomes of the program.

4 Rights in the Technical Space

Technologists are often presented as a monolithic bloc, represented first and foremost in the policy sphere by "big tech" CEOs like Mark Zuckerberg or Jeff Bezos. Internal debates within technology spaces are presented as dry, technical issues at best irrelevant to "ordinary people", and at worst deliberately condescending. This perception is not helped by how many issues hinge on arcane technical details which are not accessible without a background in often very specific fields of computer science or programming – or even of the development process itself.

While many tech activists focus on issues directly relevant to the public, such as surveillance, intellectual property, and infrastructure, one of the core elements of activism in technology spaces is

15. While a useful rhetorical example, such a program is impossible in reality due to the laws of "information entropy" – lost information cannot be recreated, only estimated, and physical limits restrict how much information about a specific event can be perfectly preserved in a finite medium.

the ideological and practical framework of *free and open source software* – which is to say, software developed and distributed according to a model that is intended to preserve the ability of the user to use the software as best suits their needs and purposes.

4.1 What is Free Software?

It is simplest to define free and open source software is to examine its opposite – so-called *proprietary* software. "Proprietary" does not simply refer to any software which is owned by some entity - it instead refers to software which has limitations imposed on the ability to modify and distribute it by users. As a general rule, software is proprietary if it is neither *free* nor *open-source*.

Free software (sometimes called "libre" software, to distinguish it from "gratis" software provided at zero cost) refers to software developed in a way that ensures or prioritises one of several ethical frameworks, which prioritise the rights of users to use and modify software to suit their purposes. *Open source software* refers to software which is developed using an open model where the source code (the human-readable instructions which are assembled into the final executable program) is distributed freely and accepts public contributions. These two categories heavily overlap in practice, with both "free software" and "open source" used as *de facto* shorthand for "free and open source software" (FOSS).

Strong insistence on "free software" is heavily associated with the Free Software Foundation, an early free software group known for maintaining the "copyleft" GNU General Public License (GPL), a free software license which places limits on distribution when used by nonfree (or insufficiently free according to the license) projects. The FSF's Free Software Definition identifies "four freedoms" for software users: the ability to run, modify, redistribute, and distribute modifications. The FSF views more permissive licenses as insignificant to protect these freedoms, while other groups see the license's restrictions and legal complexity as a barrier restricting developers and discouraging adoption of open models.[16]

16. Criticism of the FSF on non-technical grounds has also significantly alienated them from the community after the reinstatement of founder Richard Stallman as a board member in 2021. Stallman, who has long been criticised for his treatment of women and his extreme statements on sexual harassment and assault, finally resigned from both the FSF board and his MIT professorship following a series of remarks made in defense of deceased MIT professor Marvin Minsky, who was implicated by the investigation into the Jeffrey Epstein child sex trafficking ring.

Conversely, a strong insistence on the "open source" term is associated with the Open Source Initiative, which uses a separate definition that focuses more on developer principles than user freedoms, while also including stronger language about what licenses *cannot* do.[17] In practice, both the Free Software Definition and Open Source Definition describe the same license schemes with only very specific exceptions, usually due to differing interpretations of specific clauses; as such, for most organisations and people within the FOSS space, the terms are largely interchangeable, with emphasis on "free software" only when specifically drawing attention to the ethical impetus for user's rights, or on "open source software" when emphasising developer behaviours and practical benefits. Some organisations, such as Open Knowledge International, explicitly state that they treat the definitions as synonymous.

The technical breadth of the rights claimed by the free and open source model began as a consequence of the basic nature of software. While it requires a considerable amount of space and machinery to, for instance, replace the engine of an automobile, any computer capable of executing a compiled program is generally also capable of modifying that program's source code if it is available – and then executing the compiler to produce a new, executable program for that same hardware. The ability to run arbitrary programs on arbitrary hardware is a fundamental facet of modern technology, and many developers take it as a personal challenge to push perceived limits. The 1993 video game *Doom*, considered a pioneer of the modern first-person shooter genre, was released as free softwware in 1997 – leading to a frenzy of fan activity, rebuilding the game to run on a variety of platforms not supported in the original proprietary release. "Can it run *Doom*?" is a classic joking response to any new hardware announcement; the game has been successfully ported[18] to run on graphing calculators, treadmills, cars, industrial machinery, ATMs, and pregnancy tests (Leon Hurley 2021). And if it can run *Doom*, it can run a text editor and the GNU Compiler

When his reinstatement was announced, the board claimed that his remarks have been taken out of context and that his behaviour is the result of poor communication skills. Stallman's reappointment was criticised within the FSF, with numerous leadership members including then-president Geoffrey Knauth resigning in protest and several subcommittees voting to block him from returning to those bodies, and from without, with numerous FOSS groups including FSF Europe cutting all formal ties to the organisation.

17. For instance, it explicitly states that source code must be made available, and that licenses cannot discriminate against specific groups; while these are implicit conclusions from the Free Software Definition's rules, they are not explicitly stated in it.

18. Modified, either by the publisher or a third party, to run on hardware that was incompatible with the initial release.

Collection[19]

The philosophical and pragmatic motives for the adoption of a free and open source model are not within the scope of this paper. However, both models have clear limitations when applied to the rights challenges arising in the software space today. Both the Free Software Definition and Open Source Definition are designed in a context of bilateral relations between developers, who produce and/or maintain software, and users, who use and/or improve software. This view of users, which developed in the early ages of information technology, often seems overly broad outside of highly technical environments - few users see modification of software as an essential need, when modification of use cases can achieve the same result. The framing of the user as the central decision-maker also overlooks the rising power of institutional users, especially governments and multinational corporations - often building their systems on top of free and open source infrastructure.

Whether or not developers of facial recognition software make the source code of their programs to law enforcement has no bearing on the people who may face criminal charges for the output of that software, especially when their attorneys are denied any access to the program or its database, and are reliant on developer testimony only. Opening up these programs to end user modifications may actually *lower* accountability, as individual users could tailor their programs to their specific goals (and accompanying biases). It is not the user of Pegasus who faces coercion from the developer, but the human rights defenders it targets who face coercion from the user and developer alike - and would continue to face that threat were the developer to allow the user to freely run, modify, and distribute the program to others. The movement for software rights can no longer focus on the relationship between developers and users alone, because not all users are created equal.

4.2 The Right to Repair

Another human rights risk arises not from technology itself, but from the power dynamics it can create. As technology's capabities grow, they become increasingly essential for basic living, if only because the alternative uses too much time or money. Many core economic, social, and cultural

19. A free and open source software package used to compile (convert from human-readable to machine-executable) most modern programming languages.

rights increasingly rely on information technology as a vital part of the supply chain, and the COVID-19 pandemic has cast this reliance (and its inequities) into stark relief. While much of the debate has focused on access to technology, access is only part of the picture; it does not matter if a community has modern Internet and home computers or if a farmer has a top-of-the-line eco-friendly tractor if the machines break down.

As technology becomes essential, so does maintenance and repair. Manufacturers are well aware of this, and it has become an essential part of their business models - the most recent estimates[20] placed Apple's warranty program as worth $8.5 billion in revenue over the 2021 fiscal year - around 3% of the company's product revenue (Warranty Week 2021). Historically, Apple's repair manuals and equipment have been treated as company secrets, necessitating that consumers purchase Apple repair plans and go to Apple-certified technicians in order to repair their equipment. This policy was only reversed in late 2021, when Apple announced a Self Service Repair program - giving customers access to manuals (for free) and parts (for purchase at an Apple online storefront), to launch in 2022 (Apple Inc. 2021). The actual details and policy implications of this program remain to be seen - in particular, the accessibility of the Apple parts store and its costs compared to third-party components.

Security is a common justification for end-user restrictions by manufacturers. It was one of the primary pillars of Apple's argument against releasing repair manuals to consumers and its war on third-party parts - in 2014, they released a software update for iPhones which disabled the device if any "unidentified" (i.e., not sourced from Apple) hardware was detected on startup, requiring that any otherwise-functioning devices be taken to have such parts replaced by official Apple suppliers (Brignall 2016). Officially, this was to protect users from "fraudulent" devices - however, it also served as essentially a fine for using third-party services. Apple further misled customers about legal rights to replacement or refund if this error occurred, leading to a $6.6 million USD settlement in an Australian lawsuit in 2018, when they ruled that Apple had violated the Australian Consumer Law by not servicing devices repaired by a third party (Bisset 2018).

Expansion of systems built to lock down repairs have also introduced far more direct means of

20. Apple has not revealed the financial details of its warranty program as a whole, necessitating third-party estimates - in particular, the impact of protection plan sales compared to part sales.

manufacturer control over consumer-owned products. The ability of manufacturers to release online updates allows modification of product behaviour after release - regardless of what the customer wants. In October of 2021, NordicTrack (a home exercise equipment producer) released a required update to their equipments which blocks access to the system's debug mode - which customers had accessed and used in order to run third-party applications, such as viewing Netflix on their equipment's built-in display. Now, customers are unable to access extra applications and can only purchase content owned by NordicTrack's parent company - in order to get the functionality that many of them paid thousands of dollars for, customers are left needing to hack their own appliances. NordicTrack officially says that limiting OS functionality is intended as a safety measure (Burgess 2021).

Enforcing these restrictions is increasingly a technical arms race between manufacturers, who want to protect business interests they see as potentially endangered by user modifications, and users who wish to retain maximum access to their products. In order to enforce software updates, manufacturers can prevent online services from connecting to "out-of-date" devices, or even instruct devices not to operate at all if software or hardware is not up to an expected standard.

This is typically opposed by so-called "jailbreaking", a term mostly associated with small portable electronics – especially early smartphones. While this may seem to be an esoteric pursuit, reserved for technophiles, hobbyists, and malicious users and of little concern to people who "just want something that works". But if, in the words of Valve founder and president Gabe Newell[21], "piracy is a service problem" for retailers, then hacking is a service problem for manufacturers and repair services - it indicates that the manufacturer's system is not meeting the user's needs, and hacking devices has become a necessity even in some of the most essential functions of society.

John Deere has made a policy of restricting third-party software and hardware maintenance through software locks placed on tractors, forcing farmers to use John Deere-owned software to use their vehicles. This software is not only owned and licensed by Deere, its use of Deere-owned cloud services provides data to the manufacturer - which is used directly by Deere as well as sold to other agricultural companies for their own use. This data, which can be essential for farmers

21. Newell is best known as the face of Steam, a pioneer of digital software distribution that today accounts for 75% of online video game sales.

looking to maximise their yields, is then only available on the service providers' terms - limiting not only access of farmers to their own data, but large-scale analysis by government and research groups to identify ways to improve agriculture at the systems level (Horton and Kirchmeier 2020). Deere's software is so restrictive that farmers have turned to the same solution as gamers; though while the Nintendo 3DS's[22] custom firmware is a free and open source project available to anyone online, farmers need to source their firmware and tools from Eastern European black markets.

Wiens 2015 characterises John Deere's software as "a fortress" - in order to fix a simple sensor system, he had to penetrate the complex proprietary system which runs the vehicle. A part failure led to a two-day halt in operations, which can be devastating for small farmers; despite John Deere's promises of the benefits of finely-tuned precision agriculture, it doesn't mean anything if the machine won't move. Farmers have turned away from the promises of high-tech solutions to purchase older machines - which not only lack the benefits promised by manufacturers for food production, but often are built to older environmental standards, compounding climate issues which already threaten agricultural output. At the time of Wiens's attempted tractor repair, it was illegal to modify proprietary software on vehicles - unlike machine parts, software could be copyrighted, and bypassing those protections violated the Digital Millennium Copyright Act (DMCA).

Congress added an exemption to the DMCA for any software involved in operating motor vehicles later in 2015, driven in part by agricultural concerns but also by the growing role of propreitary operating systems in passenger vehicles. In response, John Deere required all customers to sign an extremely limiting license agreement which forbade them from making any otherwise-legal modifications - a move which has been compared to Monsanto's restrictions on seed replanting and crop control, also grounded in controversial copyright and patent provisions (Horton and Kirchmeier 2020). Meanwhile, an international black market has emerged online, selling cracked (software on which copy protections have been disabled or removed) copies of John Deere diagnostic tools to farmers and rural repair shops who can't access expensive manufacturer certifications and tools. When asked about this, John Deere claimed there are "no repair problems for consumers" - and that allowing software modifications would risk malfunction (Koebler 2017).

22. A handheld gaming console released in 2011 with an expansive jailbreaking/homebrew scene.

These frustrations have given rise to an unusual alliance between small farmers, technicians, and electronics activists. The so-called right to repair movement, which seeks to establish a legal right for the owner of a device to maintain and modify it as they wish, has seen a series of policy victories - and marks one of the major adoptions of a rights-based framework within the technology space. The summer of 2021 saw a rapid expansion of policies relating to repair in the United States, especially at the executive level. The Federal Trade Commission released an expansive report to the legislature on manufacturer efforts to limit repairs (FTC 2021b). This was shortly followed by an executive order from the Biden administration, which as part of a broader initiative to promote competition in the U.S. economy took specific aim at manufacturers obstructing repair efforts on their products (Duffy 2021). Finally, near the end of July, the FTC unanimously voted to strengthen enforcement against repair restrictions which violate existing antitrust laws (FTC 2021a). However, the FTC's ruling is not binding law, and repair rights in the U.S.

4.3 Placing Technical Advocacy in a Broader Human Rights Framework

The discussion of software license models and car maintenance may seem removed from issues of human rights - something which is not helped by the attitudes of many within the communit.

The typical answer to surveillance and rights concerns raised within the free and open source software community is to simply advocate switching away from proprietary systems which implement them, to free and open systems which can be publicly audited and confirmed not to. The transition is framed purely in the context of individual users, and not their broader social context; when faced with large, online services such as Facebook or the Google suite, the only solution that most groups offer is not to use them at all. Needless to say, this is not a choice most users have. In the era of centralised cloud services, protecting digital rights by changing to free and open source software is to me evocative of campaigns to stop climate change by having homeowners use marginally better lightbulbs: helpful, and superior to the alternatives, but insufficient to address the greater problems, and at worst serving as a distraction from questions of institutional responsibility or systemic failures.

Further, the primary rights championed by both the free and open source and repair communities

largely focus on issues that are only immediately relevant to technical users. Whether or not a user has access to the source code of a program to modify it is only a concern for users who have the interest and relevant knowledge to perform such modifications. Even as a programmer myself, I have only rarely found the need to modify a program at the source level to suit my own uses. The rights asserted by these movements are not tied to existing human rights frameworks directly by their advocates – but I will argue that they should be (Petrie et al. 2006).

For one prominent example, user experience design has struggled to accommodate people with disabilities – complicated on both ends by a lack of developer familiarity with (often non-standardised or proprietary) assistive devices and the difficulties in recruiting people for qualitative testing. Clint Lexa, better known by their Twitch handle "halfcoordinated", is a former video game speedrunner with a disability known as hemipareisis, restricting sensation and motion in the right half of their body. Their entire speedrunning career, including multiple world records and appearances on the "big stage" at the multi-million-dollar charity fundraising event Games Done Quick, was performed one-handed. Lexa now works for Ubisoft as an accessibile design specialist, working on improving the industry's approach to the differing needs of different players. In a 2016 interview, when asked about design considerations for limited hand usage, their response was simple: "complete freedom" over input configuration. "It's impossible to predict what everyone's situation is", so to improve accessibility, users should be able to modify the program's input settings as suits their needs (Grant 2016).

Video games are perhaps the most "inflexible" form of software when it comes to accessibility - the line between user-hostile difficulty and artistic intent is difficult to draw, and efforts to expand accessibility through customisation have faced intense blowback from elements of the community that view accessibility as a cynical marketing ploy meant to justify "dumbing down" gameplay. Despite this, games are arguably the area with the most progress; most office software, for instance, has only recently adopted basic user experience customisation such as colour customisation. Even then, it leaves users limited to those accessibility options that the developer decides to implement, and their timeline for doing so. By opening up software to more modifications, it also opens up accessibility to experts and advocates who can build the systems that their communities need

themselves, instead of relying on developers to predict every situation.

The rights asserted by technology activists are primarily discussed in their first-order context - the ability of users to modify and understand their own systems – but the logical extension of these rights is the ability of one user to modify and understand systems for the benefit of others. "Linus's law", named in honour of Linux[23] and Git[24] creator Linus Torvalds, states that "with enough eyes, all bugs are shallow": in other words, open development and engagement with a large community leads to problems being identified and repaired more quickly (Amit and Feitelson 2020). I would state a complementary law: with enough access, all use cases are significant. That is, by improving the accessibility of the internals of a program or system, more people become able to modify that system for purposes not considered by original developers — especially those for whom access was never a barrier — and in turn pass on their modifications to others.

5 Rights-Based Approaches from Policy

The predominant human rights issue in Internet policy has been the question of privacy. Privacy itself has an unusual human rights history: while the Universal Declaration of Human Rights states that no one will be subjected to "arbitrary interference with [their] privacy", a stance reiterated by the International Covenant on Civil and Political Rights, there has traditionally been little oversight or enforcement of this right. The United Nations established the first mandate for a special rapporteur on privacy only in 2015. However, privacy rights and how they relate to digital technology has been an international issue since the early days of the modern Internet.

Since the 1990s, there have been two dominant paradigms in handling personal digital information – the American model, where data transfers between third parties are permitted by default, and the European model, where they are restricted by default. This difference, embodied in the European Data Protection Directive of 1995 (EDPD), was a major point of transatlantic tension

23. A free and open source operating system kernel (essentially the core system on which all the rest of an OS is built). One Linux-based system, Android, is the most-used operating system in the world, with over 41% of global market share.

24. A version-control system designed to coordinate software development between multiple authors. According to a 2018 Stack Overflow survey of nearly 75,000 developers, 87.2% used Git for at least some projects. The second-most-used system, Subversion/SVN, was only used by 16.1%.

until the negotiation of the Safe Harbor Agreement of 2000, intended to reconcile these two different models into a single transnational legal framework. Safe Harbor codified a legal and technical structure by which American companies would comply with EU data protection laws when dealing with European data, which was deemed to provide *adequate protection* to EU residents such that data transfers from European users to Americna companies were permissible under EU law (Weiss and Archick 2016).

Safe Harbor was the dominant transatlantic data paradigm until the 2013 revelation of U.S. government surveillance programs by Edward Snowden. This program, known as PRISM, was conducted primarily by the U.S. National Security Agency (NSA), but with the cooperation of many U.S. companies – including several who were nominally bound by Safe Harbor compliance. This led to a strong pushback against Safe Harbor within the EU, and efforts by the European Council to renegotiate or amend the agreement (Woollacott 2013; European Commission 2013).

In the wake of Snowden's revelations, Max Schrems, an Austrian privacy advocate, filed a complaint with the Irish data protection authority that Facebook's transfer of his data to the US lacked adequate protection in light of NSA surveillance activities. The Irish authorities rejected the case, citing Safe Harbor, leading Schrems to appeal first to the Irish High Court - who accepted the appeal and subsequently referred the case to the Court of Justice of the European Union (CJEU) (Mac Cormaic 2014). While talks between the European Commission and U.S. government were ongoing, they made little progress as the Schrems case advanced. A European Commission lawyer stated that Brussels was unable to guarantee safeguards could be respected, and advised the best way to avoid U.S. surveillance was to "delete [your] Facebook account" (Nielsen 2015) – an echo of similar attitudes among technology activists. The CJEU would rule in October 2015 that the Safe Harbor decision was invalid, as it had enabled "interference, by United States public authorities, with the fundamental rights of persons" (CJEU 2016).

Following the Schrems decision, the EU passed a new law, the General Data Protection Regulation (GDPR), which established new rules for data processing both within Europe and for data transferred to other countries. Concurrently, it entered into negotiations with the United States, culminating in a new agreement for data transfer known as Privacy Shield. This new agreement

maintained all of the original Safe Harbor restrictions and obligations for data controllers, in addition to adding new requirements or strengthening obligations to original ones (Bryan Cave LLP 2016). The Privacy Shield agreement took hold immediately, while the GDPR would not enter into force until 2018 to allow European services to comply with its requirements.

A crucial element of the GDPR is its adoption of a much more explicit rights-based approach to user data access and control. It establishes several fundamental rights for EU residents (data subjects) with regards to personal data. Many of these rights are phrased and empowered in a very positive sense - they require states to enforce compliance with requests made according to GDPR rights, as well as to actively inform data subjects of their rights under the law. Six articles of the GDPR specifically name rights in their titles, namely the rights to access, rectification, erasure, restriction of processing, portability, and objection (Articles 15-18 and 20-21). Article 22 additionally includes a conditional right to not be subject to purely automated decisions which "significantly affect" the data subject, unless such processing is necessary by contract, the subject gives their explicit consent, or the processing is authorised by other EU or member state laws. Finally, Article 19 sets out a positive obligation for service providers (controllers) to communicate information and decisions made under other GDPR rights to anyone else who has received the data. Collectively, Articles 15-22 are considered the rights of the data subject under Article 12, which mandates that controllers act to facilitate the exercise of these rights free of charge, with possible legal penalties (European Parliament 2016).

The passage of the GDPR was lauded as a victory by privacy activists, and its entry into effect in 2018 launched a flurry of legal actions. Human Rights Watch described it as "one of the strongest and most comprehensive attempts" to regulate data use (Human Rights Watch 2018). As of the time of writing, GDPR violations have led to 1.2 billion euros in fines - a statistic dominated by a single 746 million euro fine issued to Amazon in July of 2021 (CMS, n.d.; Shead 2021). It has become a standard of comparison for data privacy laws in other jurisdictions, such as the California Consumer Privacy Act (CCPA) and its successor the California Privacy Rights Act (CPRA) (Lucarini 2020; Sarian 2020).

Despite these advances in digital privacy rights, there has been a coordinated counterpush by

governments concerned about the impact on law enforcement and national security. The gradual reversal of privacy rulings from the European Court of Human Rights is paralleled by efforts from national governments to either introduce exemptions to GDPR protections for law enforcement, or to simply bypass the court entirely (Kayali 2021).

6 Moving to Open Technology Governance

Where the free and open source movement focuses on users as contributors, the GDPR and related policies focus solely on users as consumers. Neither reflects the full scope of technology's role in society.

Technology activists – driven in part by the American-style individualism of establishment FOSS figures such as the FSF's Richard Stallman and OSI's Eric S. Raymond – have largely not reached out to global human rights spaces. Some groups have worked to bridge this gap; the Organisation for Ethical Source, founded by FOSS contributors concerned with accessibility and equity within the movement, has seen many prominent open source projects adopt their Contributor Covenant, an open-source code of conduct (both in the sense of being developed using an open-source model, and the sense of describing open-source projects) intended to address common criticisms of the culture of the free software movement. However, while the OES's Covenant has seen success, their actions remain largely focused on the internal culture of the movement and not its relationship with broader human rights spaces.

Another limit of the technical approach is the relationship between software *development* and software *operations*. Where the former is the development and maintaining of a program, the latter is the use of that program – especially when run as a service for a separate group of users. The two are often grouped together (and shortened to "devops"), especially when dealing with large-scale services at scale. IT staff for large organisations often maintain and operate software simultaneously – especially as much underlying infrastructure runs on open-source systems which allow for closer integration of development and operations. However, in the rights space, either development or operations alone can be of concern; the developers of an open database program have no control

over that program being adapted to a tool of public mass surveillance, and the users most vulnerable to such surveillance cannot simply adapt the program to no longer invade their privacy.

While I personally believe that the model has both practical benefits and ethical significance, it is unlikely that limiting official use of software to only programs which are developed according to the free, open-, and ethical-source model is either politically or technically feasible in the foreseeable future. Nor is it viable to shift services to an open operations model – especially in the case of machine-learning algorithms, where truly transparent, publically auditable operations would require access to training data, which could itself raise privacy concerns. Nor is this model of development and operations alone sufficient to guarantee that software is used ethically; while the developer has some sway over what a technology can and can't do, the final usage of a technology rests with the user. Much as chemicals developed to improve agricultural yields became horrifying chemical weapons over the course of the 20th century, the developer's intentions can only go so far; in the language of systems theory, "the purpose of a system is what it does" – not what it was intended to do.

Perhaps my favourite quote on the matter comes from G.H. Hardy, one of the great early 20th century mathematicians. Hardy, like many of his colleagues, was a staunch anti-war advocate, and despised the means by which scientific discoveries had been militarised. His 1940 essay *A Mathematician's Apology*[25] (Hardy 1940), discusses the potential of harm by mathematics – "There is one comforting conclusions which is easy for a real mathematician. Real mathematics has no effects on war. No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity[26], and it seems very unlikely that anyone will do so for many years." In hindsight, Hardy could not have picked a worse pair of examples.

A Mathematician's Apology was published in November of 1940. A little over a year prior, on September 4, 1939, a little-known mathematician named Alan Mathison Turing reported for duty at the Government Code and Cipher School's campus at Bletchley Park. Turing was the epitome

25. "Apology" is used here in the sense of apologetics or religious apologism, the formal defense of a belief or doctrine – in this case, the defense of Hardy's view of "pure" mathematics's value as an art and philosophy to a world who valued it first and foremost for its material applications.

26. The distinction between mathematics and physics was still in flux in Hardy's time – Einstein was considered a mathematician, not a physicist, as his work was theoretical in nature.

of what Hardy would call a "real mathematician", and it was his work in the theory of numbers that would be the focus of his efforts in the Second World War – the development of modern cryptanalysis. All modern ciphers trace themselves to Turing's work, with pre-Turing systems (referred to collectively as "classical" cryptography) essentially rendered completely irrelevant for anything besides as a teaching tool. War had found its use for the theory of numbers, and it would profound implications in peace. Turing's work led to him being named the father of computer science – though the field would not come into its own until well after his suicide in 1954.[27]

As for the theory of relativity, its most terrifying implication was unleashed upon the city of Hiroshima on the 6th of August, 1945.[28]

Hardy was not speaking from a position of ignorance; he was a brilliant mathematician, and intimiately familiar with what relativity and number theory were to mathematicians of his time. But times change, and science, technology, and human knowledge are growing faster than ever before. Developers and inventors cannot account for every use of their technology. Operators cannot account for every change in the circumstances of users. Users cannot account for the impacts of every possible future technology on their lives and their rights. Any solution that places the responsibility solely on one of these groups will never truly address the challenges of emerging technology.

If policy is slow to respond to changes in technology, technology will gladly set policies of its own. Lessig's declaration that "code is law" disturbed the developers of the 1990s, who did not see themselves as policymakers; today's technology firms take it for granted. Policymakers need to learn a broader lesson – if code is law, law is always subject to interpretation and debate. How we use the code shapes the law as much as the code itself – but we cannot ask judges to interpret a law that they cannot read. As more of our social functions become reliant on technology, that technology must in turn be more accessible and comprehensible to policymakers, jurists, and the

27. Turing was persecuted for his homosexuality, leading to judicially mandated chemical castration, which came with significant side-effects that may have led to his death. The British government officially apologised for Turing's treatment in 2009, and he received a posthumous royal pardon in 2013. Other men convicted under these laws were collectively pardoned by Parliament in 2017, though only in England and Wales.

28. Contrary to the popular portrayal of Einstein's equation $E = mc^2$ denoting the amount of energy unleashed by a nuclear bomb, a more accurate formulation would be $E = (\Delta m)\, c^2$, as only a small amount of total input mass is converted to energy by the reaction. The estimated yield of the weapon that destroyed Hiroshima was 63 terajoules, which corresponds to the conversion of 701 milligrams of mass – around 28% of the mass of a typical US penny.

general public alike. Much as an artificial intelligence system uses its best approximation of a face to reconstruct an identity, placing legal weight on software from only an approximation of its inner workings risks creating an artificial jurisprudence – the "laws of code" being written, interpreted, and executed by an opaque, unaccountable system without any checks or balances to protect human rights.

References

Amit, Idan, and Dror G. Feitelson. 2020. "The Corrective Commit Probability Code Quality Metric." *CoRR* abs/2007.10912. arXiv: 2007.10912. https://arxiv.org/abs/2007.10912.

Apple Inc. 2021. "Apple announces Self Service Repair." Apple Inc., November 17, 2021. Accessed November 23, 2021. https://www.apple.com/newsroom/2021/11/apple-announces-self-service-repair/.

Bisset, Jennifer. 2018. "Apple fined $6.6M in Australia after Error 53 controversy" (June 18, 2018). Accessed November 12, 2021. https://www.cnet.com/tech/mobile/apple-bricked-our-phones-with-error-53-now-it-owes-6-8-million-in-australia/.

Brignall, Miles. 2016. "'Error 53' fury mounts as Apple software update threatens to kill your iPhone 6" (February 5, 2016). Accessed November 12, 2021. https://www.theguardian.com/money/2016/feb/05/error-53-apple-iphone-software-update-handset-worthless-third-party-repair.

Bryan Cave LLP. 2016. "A Side-by-Side Comparison of "Privacy Shield" and the "Safe Harbor"." Bryan Cave LLP, July 16, 2016. Accessed October 6, 2021. https://iapp.org/media/pdf/resource_center/Comparison-of-Privacy-Shield-and-the-Safe-Harbor.pdf.

Burgess, Matt. 2021. "Locked Out of 'God Mode,' Runners Are Hacking Their Treadmills" (November 19, 2021). Accessed November 23, 2021. https://www.wired.com/story/nordictrack-ifit-treadmill-privilege-mode/.

Christakis, Theodore, and Katia Bouslimani. 2019. "National Security, Surveillance, and Human Rights." *Oxford Handbook on the International Law of Global Security* (December 1, 2019). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3599994.

CJEU. 2016. "The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid." Court of Justice of the European Union, October 6, 2016. Accessed October 3, 2021. https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

CMS. n.d. "GDPR Enforcement Tracker." CMS. Accessed October 6, 2021. https://www.enforcementtracker.com/?insights.

Cyphers, Bennett, Adam Schwartz, and Nathan Sheard. 2021. "Face Recognition Isn't Just Face Identification and Verification: It's Also Photo Clustering, Race Analysis, Real-time Tracking, and More." Electronic Frontier Foundation, October 7, 2021. https://www.eff.org/deeplinks/2021/10/face-recognition-isnt-just-face-identification-and-verification.

Davies, Nick. 2008. "The bloody battle of Genoa." *The Guardian* (July 16, 2008). https://www.theguardian.com/world/2008/jul/17/italy.g8.

Duffy, Claire. 2021. "Biden's executive order takes on right-to-repair. It could make fixing your smartphone easier" (July 14, 2021). Accessed November 8, 2021. https://www.cnn.com/2021/07/14/tech/right-to-repair-biden-executive-order/index.html.

"Enough is enough! - NSO Group." n.d. NSO Group. Accessed February 5, 2022. https://www.nsogroup.com/Newses/enough-is-enough/.

European Commission. 2013. "European Commission calls on the U.S. to restore trust in EU-U.S. data flows," November 27, 2013. Accessed October 4, 2021. https://ec.europa.eu/commission/presscorner/detail/en/IP_13_1166.

European Parliament. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016." European Union, April 27, 2016. Accessed October 2, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Fisher, Phineas. 2016. "Hack Back! A DIY Guide." Translated by Jared Burrows. Content warning: In keeping with tongue-in-cheek hacker sensibilities, the paper begins with an ASCII art rendition of a cartoon character urinating on a HackingTeam logo. April 18, 2016. https://gist.github.com/jaredsburrows/9e121d2e5f1147ab12a696cf548b90b0#file-gistfile1-txt-L864.

FTC. 2021a. "FTC to Ramp Up Law Enforcement Against Illegal Repair Restrictions." U.S. Federal Trade Commission, July 21, 2021. Accessed November 8, 2021. https://www.ftc.gov/news-events/press-releases/2021/07/ftc-ramp-law-enforcement-against-illegal-repair-restrictions.

———. 2021b. "Nixing the Fix: An FTC Report to Congress on Repair Restrictions." U.S. Federal Trade Commission, May. Accessed November 8, 2021. https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf.

Gavarrete, Julia, Daniel Reyes, and Óscar Martínez. 2022. "22 Members of El Faro Bugged with Spyware Pegasus." *El Faro* (January 12, 2022). https://elfaro.net/en/202201/el_salvador/25936/22-Members-of-El-Faro-Bugged-with-Spyware-Pegasus.htm.

Grant, Chris Daniel. 2016. "How a gamer with a disability speedruns some of the world's fastest games," January 6, 2016. https://www.polygon.com/2016/1/6/10723150/agdq-2016-halfcoordinated-speedrun-disabled-gaming.

Grother, Patrick, Austin Hom, Mei Ngan, and Kayee Hanaoka. 2021. *Face Recognition Vendor Test (FRVT) Part 7: Identification for Paperless Travel and Immigration* [in en], July 13, 2021. https://doi.org/https://doi.org/10.6028/NIST.IR.8381. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932484.

Grother, Patrick, Mei Ngan, and Kayee Hanaoka. 2019. *Face Recognition Vendor Test Part 3: Demographic Effects.* Technical report. December 19, 2019. https://doi.org/10.6028/nist.ir.8280. https://doi.org/10.6028/nist.ir.8280.

Hardy, G.H. 1940. "A Mathematician's Apology." *Cambridge University Press* (November).

Hill, Kashmir. 2020. "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match." *The New York Times* (November 29, 2020). https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

Holden, Michael, and Andrew Macaskill. 2021. "Sheikh Mohammed ordered phones of ex-wife and lawyers to be hacked: UK court." *Reuters* (October 6, 2021). https://www.reuters.com/world/middle-east/dubais-sheikh-mohammed-ordered-phones-ex-wife-lawyers-be-hacked-uk-court-says-2021-10-06/.

Horton, Thomas J., and Dylan Kirchmeier. 2020. "John Deere's Attempted Monopolization of Equipment Repair, and the Digital Agricultural Data Market - Who Will Stand Up for American Farmers?" *CPIO Antitrust Chronicle* (January). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3541149.

Human Rights Watch. 2018. "The EU General Data Protection Regulation: Questions and Answers," June 6, 2018. Accessed October 7, 2021. https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation.

IATA. 2018. "Biometric Boarding using Identity as a Service: The potential impact on liability in the aviation industry." International Air Transport Association, July. Accessed February 5, 2022. https://www.iata.org/contentassets/1f2b0bce4db4466b91450c478928cf83/biometric-boarding-white-paper-final-v3-1.pdf.

———. 2021. "Passengers Want to Use Biometrics to Eliminate Queuing Post Pandemic." International Air Transport Association, November 15, 2021. Accessed February 5, 2022. https://www.iata.org/en/pressroom/2021-releases/2021-11-15-01/.

Kayali, Laura. 2021. "France seeks to bypass EU top court on data retention." Politico, March 3, 2021. Accessed October 7, 2021. https://www.politico.eu/article/france-data-retention-bypass-eu-top-court/.

Koebler, Jason. 2017. "Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware" (March 21, 2017). Accessed November 13, 2021. https://www.vice.com/en/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware.

Kushner, David. 2016. "Fear This Man." *Foreign Policy* (April 26, 2016). https://foreignpolicy.com/2016/04/26/fear-this-man-cyber-warfare-hacking-team-david-vincenzetti/.

Leon Hurley, Joe Donnelly, Heather Wald. 2021. "15 things that prove that DOOM will run on literally anything." Input Magazine, October 15, 2021. https://www.gamesradar.com/12-things-that-prove-that-doom-will-run-on-literally-anything/.

Levinson, Chaim, Amos Harel, and Yaniv Kubovich. 2018. "Khashoggi's Friend Sues Israel's NSO: Spyware That Hacked My Phone Had Major Role in Murder." *Haaretz* (December 3, 2018). https://www.haaretz.com/israel-news/.premium-khashoggi-associate-sues-israeli-cyber-firm-nso-had-major-role-in-murder-1.6704486?lts=1644183670735.

Lucarini, Francesca. 2020. "The differences between the California Consumer Privacy Act and the GDPR." Advisera, April 13, 2020. Accessed October 6, 2021. https://advisera.com/eugdpracademy/blog/2020/04/13/gdpr-vs-ccpa-what-are-the-main-differences/.

Mac Cormaic, Ruadhán. 2014. "High Court refers Facebook privacy case to Europe," June 18, 2014. Accessed October 3, 2021. https://www.irishtimes.com/business/technology/high-court-refers-facebook-privacy-case-to-europe-1.1836657.

Marczak, Bill, and John Scott-Railton. 2016. "The Million Dollar Dissident." University of Toronto, August 24, 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Ni Loideain, Nora. 2020. "The Approach of the European Court of Human Rights to the Interception of Communications." *EU Data Privacy Law and Serious Crime* (September 25, 2020). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3699386.

———. 2021. "Not So Grand: The Big Brother Watch ECtHR Grand Chamber judgment." Information Law and Policy Centre, May 28, 2021. Accessed December 7, 2021. https://infolawcentre.blogs.sas.ac.uk/2021/05/28/not-so-grand-the-big-brother-watch-ecthr-grand-chamber-judgment/.

Nielsen, Nicolaj. 2015. "EU-US data pact skewered in court hearing," March 25, 2015. Accessed October 4, 2021. https://euobserver.com/justice/128131.

O'Neill, Patrick Howell. 2019. "The fall and rise of a spyware empire." *Technology Review* (November 29, 2019). https://www.technologyreview.com/2019/11/29/131803/the-fall-and-rise-of-a-spyware-empire/.

"Pegasus Project: Macron among world leaders selected as potential targets of NSO spyware." 2021. Amnesty International, July 20, 2021. https://www.amnesty.org/en/latest/news/2021/07/world-leaders-potential-targets-of-nso-group-pegasus-spyware/.

Petrie, Helen, Fraser Hamilton, Neil King, and Pete Pavan. 2006. "Remote Usability Evaluations With Disabled People." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 1133–1141. CHI '06. Montréal, Québec, Canada: Association for Computing Machinery. ISBN: 1595933727. https://doi.org/10.1145/1124772.1124942. https://doi.org/10.1145/1124772.1124942.

Sajfert, Juraj. 2021. "The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of privacy?" European Law Blog, June 8, 2021. Accessed December 7, 2021. https://europeanlawblog.eu/2021/06/08/big-brother-watch-and-centrum-for-rattvisa-judgments-of-the-grand-chamber-of-the-european-court-of-human-rights-altamont-of-privacy/.

Sarian, Ronald. 2020. "Californians take another step toward European-style privacy protection with the CPRA." Constangy, Brooks, Smith & Prophete, LLP, November 24, 2020. Accessed October 6, 2021. https://www.jdsupra.com/legalnews/californians-take-another-step-toward-15883/.

Saudelli, Giulia. 2021. "Opinion: Fascism still rears its ugly head in Italy." *Deutsche Welle* (October 12, 2021). https://www.dw.com/en/opinion-fascism-still-rears-its-ugly-head-in-italy/a-59483231.

Shead, Sam. 2021. "Amazon hit with $887 million fine by European privacy watchdog." CNBC, July 30, 2021. Accessed October 6, 2021. https://www.cnbc.com/2021/07/30/amazon-hit-with-fine-by-eu-privacy-watchdog-.html.

Stokes, Elaisha. 2020. "Wrongful arrest exposes racial bias in facial recognition technology." *CBS News* (November 19, 2020). https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/.

Warranty Week. 2021. "Apple's Product Warranties & Applecare." Warranty Week, November 4, 2021. Accessed November 12, 2021. https://www.warrantyweek.com/archive/ww20211104.html.

Watson, Craig, Gregory Fiumara, Elham Tabassi, Su Cheng, Patricia Flanagan, and Wayne Salamon. 2015. *Fingerprint Vendor Technology Evaluation* [in en], January 8, 2015. https://doi.org/https://doi.org/10.6028/NIST.IR.8034.

Weiss, Martin A., and Kristin Archick. 2016. "U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield." Congressional Research Service, May 19, 2016. Accessed October 3, 2021. https://sgp.fas.org/crs/misc/R44257.pdf.

Wiens, Kyle. 2015. "New High-Tech Farm Equipment is a Nightmare for Farmers" (February 5, 2015). Accessed November 13, 2021. https://www.wired.com/2015/02/new-high-tech-farm-equipment-nightmare-farmers/.

Williams, Robert. 2021. "I Did Nothing Wrong. I Was Arrested Anyway." American Civil Liberties Union, July 15, 2021. Accessed April 15, 2022. https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway.

Woollacott, Emma. 2013. "EU to vote on scrapping 'Safe Harbor' data rules." Forbes, December 18, 2013. Accessed October 4, 2021. https://www.forbes.com/sites/emmawoollacott/2013/12/18/eu-to-vote-on-scrapping-safe-harbor-data-rules/.