ACIG APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Utopia Lost – Human Rights in a Digital World

Received: 13.10.2022
Accepted: 29.11.2022
Published: 03.12.2022

Aaron Brantly Department of Political Science, Tech4Humanity Lab, Hume Center for National Security and Technology, Virginia Tech, USA, ORCID: 0000-0003-4193-3985

Abstract

The long progress towards universal human rights is regressing. This regression is pronounced within digital spaces once thought to be potential bulwarks of a new era in human rights. But on the contrary, new technologies have given rise to threats that undermine the autonomy, empathy, and dignity of human beings. Early visions of human rights being strengthened by networked technologies have instead crashed into technological realities which not only fail to advance human rights discourses, but rather serve to actively undermine fundamental human rights in countries around the world. The future of human rights is increasingly threatened by advances that would make George Orwell blush. Omnipresent data collection and algorithmic advances once promising a utopian world of efficiency and connection are deeply interwoven with challenges to anonymity, privacy, and security. This paper examines the impact of technological advances on the regression of human rights in digital spaces. The paper examines the development of human rights through changes in concepts of autonomy, empathy, and dignity, it charts their regression as technologies are used to increasingly prey on these very same characteristics that undergird human rights discourses.

Keywords

artificial intelligence, cybersecurity, governance, human rights, privacy

1. Introduction

Human rights as a concept have progressed substantially over the last 100 years. From the Universal Declaration of Human Rights (1948), the signing of the post war Geneva Conventions (1949), and multiple national constitutions, and laws enacted by states and unions of states there has been a drive to expand and protect human rights. The recognition and protection of these rights has proceeded unevenly over the last 80 years. The inconsistent safeguarding of human rights has been undermined or ignored in a variety of political and social contexts in nearly every state. Yet where these rights seek to establish a robust ground upon which to base fundamental rights inherent to all humans, the advances of networked technologies have provided a new and pervasive means by which states can, with high degrees of efficiency, erode rights once

Cite this article as:
A. Brantly, "Utopia Lost – Human Rights in a Digital World," ACIG, vol. 1, no. 1, 2022, DOI: 10.5604/01.3001.0016.1238

Corresponding author:
Aaron Brantly, Department of Political Science, Tech4Humanity Lab, Hume Center for National Security and Technology, Virginia Tech, USA, ORCID: 0000-0003-4193-3985; E-mail: abrantly@vt.edu

normatively and legally established. Networked technologies that were once believed critical to ushering in a more just world respectful of the rights of human beings, have instead been co-opted to surveil, censor, and constrain rights. While utopia was never a reality, this loss of rights, and the shifting of the normative frameworks on human rights, represents a lost vision of a utopia in which the rights and dignity of humans could have been. The analysis below is constrained to digital human rights violations whose attributes undermine human autonomy, empathy, and dignity.

Alexander Wendt is famous for his constructivist turn of phrase "anarchy is what states make of it"[1]. Similarly, the development of the norms and ideas surrounding the conceptualization of human rights are what states make of them. Nearly a century of progress towards the rights of human beings is being undermined through the slow alteration of the ideational and normative constructs about what constitutes rights and who should and can respect those rights. Whereas the development of human rights followed an often painfully slow process of norm evolution through an ever-progressing norm life cycle [2], that cycle never completed, and the internalization of human rights norms in nearly all states has begun to reverse itself. This reversal was forecast by a few scholars, notably by Ron Deibert in a series of volumes examining the encroachment of the state through the utilization of digital means to undermine human rights [3–5]. Subsequent research on the rate of change indicates that the speed of reversion away from a recognition of human rights in digital spaces correlates with the rate of change in digital capabilities developed by states [6]. Early concerns about the impacts of technological advances in networked technologies centered on authoritarian regimes [7]. Despite informed warnings about authoritarian counter movements utilizing technology to undermine the advances of norms on human rights, many in the academic and policy communities professed a profound and not entirely unwarranted optimism about technology and its power to enable human rights[1]. Among the scholars who led both the academic and policy discussions on the ability of technology to facilitate human rights was Larry Diamond, who in writing on the application of technology to civil and political rights spoke of the potential for technology to "liberate" and empower individuals [8]. The empowerment vision often correlated with technological advance is not without merit. There is substantial evidence that networked technologies enabled social mobilizations to challenge authoritarian and rights abusing states and state institutions [9, 10]. Yet these challenges were often met by the counter usage of networked technologies for highly repressive and intrusive digital surveillance and manipulation [11].

Ron Deibert and the Citizen Lab at the University of Toronto have been instrumental in identifying and bringing to public consciousness a variety of violations of human rights norms [12, 13]. Deibert in particular, has been outspoken in highlighting what he identifies as the need for a "reset" in the balance between, on the one hand, implementation and use of technology, and on the other, human needs [14]. The stories of human rights and digital rights have not transpired in isolation. They are intrinsically enmeshed. Organizations ranging from Amnesty International, Human Rights Watch, Doctors without Borders, and others have increasingly joined digitally oriented rights organizations such as the Electronic Frontier Foundation, Access Now and many more in a common push to secure human rights in digital spaces. In truth, rights defended in digital spaces are not meaningfully distinct from those same rights expressed in non-digital spaces. And very often violations of rights in digital spaces occur in tandem with human rights violations in physical spaces.

Despite human rights violations in digital and physical spaces being highly correlated, the rights within the two spheres do not carry with them the same normative value. The result is that rights, once freely exercised through digital means, are increasingly undermined as state capacity to control digital spaces has increased. Yet the restriction of rights is not solely the result of states recapturing rights once previously held. They are aided in their capture by a range of actors who, using the market and the

[1] A large volume of research is available on the early positive benefits and some challenges associated with new technologies and human rights. The works listed here are but some of many that express substantial optimism about the role technology can play in facilitating human rights [110–115].

means of surveillance capitalism [15], alter the norms associated with digital human rights more broadly. The result is a subtle yet profound shift in concepts of free speech, privacy, and surveillance to name just a few of the broader spectrum of rights impacted.

This work contextualizes the formation of digital human rights within the larger and comparatively more robust history of human rights outside of digital spaces. Examining the construction of norms associated with the formation and subsequent decline of rights in digital spaces through a constructivist lens, this work answers the questions 'How?' and 'Why?' digital rights are regressing despite increasing advances in networked technologies once heralded as tools of human rights empowerment. The work proceeds below in four sections. The first defines both human rights and norms, it provides a brief history of the construction of human rights norms. The second section examines the rise of digital rights and the utopian views associated with rapidly advancing networked technologies. The third section examines the decline of rights in digital spaces in the context of a failure to solidify norms around digital rights in relation to human rights. The final section provides a discussion on the loss of rights and the path forward for digital rights norm entrepreneurs.

2. Constructing Conventional Human Rights

Human rights are a modern concept within the Western political cannon. On the origins of human rights Lynn Hunt notes "Human rights are difficult to pin down because their definition, indeed their very existence, depends on emotions as much as on reason" [16]. Hunt's implication of the emotional attributes resident in human rights is indeed central to what amounts to a constructivist argument which she develops over the course of her work. She isolates a core tenet of human rights that this work seeks to develop in greater detail, concepts of perception concerning both the self and other, and the recognition of a simultaneous uniqueness and universality of thought and condition. The development of these concepts into an applicable and meaningful body of cultural and societal knowledge and identity is constitutive. Hunt specifically and parsimoniously identifies the concepts of autonomy and empathy as critical to the constitution of norms on what would eventually evolve into human rights. It is important to note that human rights framed in such a way as to privilege the autonomy of individuals, i.e. individualism, is not culturally universal and has implications in non-western societies. Yet, to set a starting point, this paper emphasizes the concepts of individuality and empathy as a basis for understanding how human rights are conceived in physical spaces, and how these same rights fail to carry over into digital spaces. It is also important to underscore advances in philosophical understandings of human life and value. In particular, and often related to the notion of individual autonomy and empathy, is the concept of dignity outlined by Immanuel Kant [17]. Kant bridged the concept of autonomy with dignity in writing "Autonomy is therefore the ground of the dignity of human nature and of every rational nature." [18]. Yet a deepening understanding of the concept of dignity into the broader field of human rights did not occur quickly.

Converting autonomy, empathy, and dignity from abstract concepts into codified legal structures was not straightforward. While enlightenment thinkers debated concepts of humanity, moral and ethical behaviors, and western authors and artists probed the mind of the individual and their unique visual appearance [16], these concepts were in opposition to millennia of lived and learned experience. Constructing identities encompassing such concepts required shifts in social, cultural, economic, political, religious, and other framings. Two areas that helped to facilitate new identities were shifts in both philosophical and artistic works which served as something akin to fuzzy norm entrepreneurship. I deliberately use the term fuzzy[2] because unlike many modern norm entrepreneurs the concepts surrounding human rights were not codified in a manner that allowed for specificity, nor were they advanced in most instances by a single group. Rather there remained only the notion that the order as it existed was not as it might be.

[2] My use of fuzzy norms contrasts with that of [116] in which states deliberately fail to define the parameters of a norm. By contrast norms here are "fuzzy" simply because they have not been articulated in a universally applicable manner in line with current cultural or societal power structures.

Specific political philosophers, such as Mary Wollstonecraft [19], pushed back on the early formulations of rights assigned to men implicitly or explicitly in law, and implicitly in works designed to further the formation of new identities rooted in rights-based discourses [20, 21]. Despite a fervent discourse that permeated reading circles on both sides of the Atlantic, initial implementations of these identity constructs for rights were entirely focused on emphasizing the propertied white male class. The most famous documents in the modern western cannon, such as the US Declaration of Independence, formally established "rights" in official documentation through the words: "We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness"[3]. These words expressed the ideals of changing social and cultural norms within existing entrenched power hierarchies. The result was the generation of rights for some and the often-brutal withholding of rights from others[4]. The concept of privileged access to rights will return in later sections. Subsequent attempts, such as the Declaration of the Rights of Man and of the Citizen (1789), similarly advanced broader concepts pertaining to human rights, yet their implementation, both in domestic environments and in colonial possessions, remained highly entrenched in systems that deliberately sought to deny rights to overwhelming majorities of inhabitants.

The fundamental development of human rights as a concept has historically also privileged the political and social rights of individuals rather than basic economic rights[5]. The separation of the economic from the social and political plays a part in the story of the regression of rights in the digital age. Yet it also influences a broader understanding of human rights in the western political context. The development of human rights is non-linear, just as all normative advances are by and large non-linear. The literature is replete with examples of the asymmetric application of human rights based on any number of factors encompassing race, class, religion, and many other attributes. Eric Weitz's *A World Divided highlights many of the inherent tensions and juxtapositions of rights within a range of communities from Namibia to Minnesota, to Brazil and Haiti* [22]. Weitz identifies that when individuals are not conceived of as belonging to a state, with citizenship, they have been historically exposed to the worst forms of degradations [22]. Arendt, writing at the end of the Second World War, identified being "stateless" as one of the worst conditions imaginable, a condition only marginally better than physical annihilation [23].

It took the cataclysm of the Second World War to begin altering social and political reality towards a more universalized understanding of Human Rights. The Universal Declaration of Human Rights (UDHR) ratified on December 10th, 1948, was pushed forward by norm entrepreneurs led by Eleanor Roosevelt in the aftermath of millions of deaths at a time when many European powers were advancing towards or experiencing colonial collapse. In many ways the UDHR arrived at what John Kingdon would refer to as a "policy window" considered as an important opening for agenda setting [24]. Work undertaken by activists, political philosophers, politicians, and many other actors capitalized on the human tragedy of war to draw together a codified understanding of human rights. Lest there be any doubt as to the reality of such a policy window being fostered by the tragedy of war, it is important to remember that prior to World War II the term "human rights" was not used with any measurable frequency [25].

The first article of the UDHR plainly states: "All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood" [26]. This statement, while inherently gendered in its formulation, ties together the concepts of autonomy, dignity, and empathy. The application of these rights, while declared universal, were in practice selective[6]. Moreover, the protection of the outlined rights was left to states. The concept of dignity as expressed in the UDHR is best explained by political philosopher Jürgen Habermas, who writes that human dignity serves as the "conceptual hinge" linking the "internalized rationally justified morality anchored in the individual conscience" of Kant and the

[3] https://www.archives.gov/founding-docs/declaration-transcript.

[4] In the case of the US Articles of Confederation and later the US Constitution numerous caveats are made to exclude persons and reduce both their individuality – independence and uniqueness – black men were considered 3/5s a man, women and non-propertied males were excluded.

[5] See for a detailed analysis of the tradeoffs associated with an emphasis on political and social rights rather than economic rights [117].

[6] Many states sought exemptions or explicitly denied rights to persons within their jurisdictions. This was true in practice with nearly every western state which became a signatory to the UDHR.

"coercive, positive, enacted law" of modern states [27]. The UDHR constitutes the output of hundreds of years of progress in fusing recognition of the autonomy, empathy, and dignity of human beings with the legal mechanisms of states capable of enforcement. Despite its monumental success in establishing a relative normative consensus on what constitutes human rights, the UDHR was not enforceable without the consent of nations. Where normative consensus arose conceptually, the translation of the concepts to applications was undertaken in piecemeal fashion by nations through their "obligations" to the ideals established in the UDHR.

This state centric approach to human rights is rooted in the sovereign rights of states established in a post-Westphalian order and presents a paradox for the protection of rights. The principal violator of rights is also obliged to be the protector of those same rights [25]. Unlike the fuzzy formation of concepts pertaining to autonomy, empathy, and dignity, developed over nearly two centuries, the emergence of increasingly powerful norm entrepreneurs capable of forming both state and non-state-based organizations to further advance norms pertaining to human rights occurred in the period after the signing of the UDHR. Although the broadest and furthest reaching statement of human rights was the UDHR, it was quickly followed by the Genocide Convention (1948), Refugee Convention (1951), Discrimination in Employment Convention (1960), Racial Discrimination Convention (1965), the Economic, Social and Cultural Rights Covenant (1966), the Civil and Political Rights Covenant (1966), the Discrimination against Women Convention (1979), the Convention against Torture (1984), the Children's Convention (1989), the Indigenous and Tribal Peoples Convention (1989), the Convention on Migrant Workers (1990), the Convention on Persons with Disabilities (2006), and the Declaration on the Rights of Indigenous Peoples (2007). This multitude of conventions and declarations arose in tandem with a rapid increase in organizations dedicated to fighting for and exposing human rights violations globally as well as within nations. Although the first major international rights organizations such as the International Federation of Human Rights (FIDH) predate the UDHR, it was in the post-World War II era where organizations such as the FDIH, the International Commission of Jurists (1952), and later Amnesty International (1961), Human Rights First (1978), Human Rights Watch (1978), and others began to emerge and exert increasing pressure on states to adhere to their commitments under international law.

Although progress has been made on both conceptualizing and enforcing human rights norms, norm violations are a regular occurrence. A substantial body of literature has examined the development of norms pertaining to human rights [28–31]. The findings are mixed, they provide a range of explanations as to how early norms on human rights emerged [28, 32], why states violate human rights [31], and why they adhere to human rights [31]. Yet despite many failings, there has been substantial progress on human rights norms [33]. The evolution from Hunt's historical framing of autonomy and empathy, to Kant's initial definitions of human dignity, onward to the flawed and often hypocritical declarations of "Independence" and the "Rights of Man" to the emergent post war policy window making possible the codification of a substantial foundation for human rights in the UDHR, has been followed by 70 years of rapid norm emergence up to the present. This situation has been fostered by an ever-growing cohort of states and NGOs that have raised established human rights as being integral to the lexicon of international politics. Imperfections and failings abound. Yet the literature, and the wider policy discourse on human rights, indicate that it has found a steady body of norm entrepreneurs willing to continue advancing it forward often in the face of great hardships.

In the last 30 years a subset of human rights emerged as an addendum to those rights previously fought for and often enumerated. Digital rights once discrete and thought the purview of a select few in connected western nations have increasingly become intertwined in all forms of human rights. Digital Rights are human rights and in the next section I briefly trace the emergence of norms and challenges emanating

through networked technologies. These norms are framed in such a way as to identify how they impact the concepts of human autonomy, dignity, and empathy. Constructing the framing of norms around these concepts is rooted in an ontological notion, i.e. the state of being of rights, outlined above, leading to the establishment of rights that form a recognition of individual human autonomy, both internally and externally identified and respected through empathy, and codified in the complex concept of dignity developed by both Kant and Habermas. Autonomy and empathy are constituent parts of the larger meta-concept of human dignity. When combined these three concepts underpin the creation of what are considered human rights. Understanding how technologies influence both the constituent components and the broader overarching concept establishes how human rights are affected by digital technologies.

3. The Rise of Digital Rights

The history of the Internet and its associated technologies has been well researched [34, 35]. The transition from circuit-switched to packet-switched data [36], followed by advances in networking large and expensive computers with Interface Messaging Processors (IMPs) [37], and eventually protocol and software suites such as the Transmission Control Protocol/Internet Protocol (TCP/IP) [38] is a socio-technical story of development that occurs within both civilian and military environments. The development of networked technologies is imbued with the hopes and fears, constraints and freedoms associated with the times in which it was initially developed. Early governance of the Internet was partially conducted through the development of the Request for Comment (RFC) process which reinforced a technocratic approach that was later to be enshrined in the nascent but developing governance structures of the Internet, including what has now become the Internet Society. The technocratic nature of the Internet often overlooked or under-estimated its expanding power and reach.

Early Internet development was hamstrung by government regulation, both from the National Science Foundation [39] and the International Traffic in Arms Regulations (ITAR) managed by the Department of State [40]. ITAR restrictions pertaining to the use of the evolving network were particularly contentious, they dealt with what can be best described as an early debate over individual rights in digital spaces. The debate led to what is commonly referred to as the first crypto war [41]. During the crypto wars of the early 1990s members of the Intelligence community and in particular the Federal Bureau of Investigation (FBI) took a strong position against allowing the commercial use of cryptography [42]. At the time of the initial fight the justification against allowing public use of cryptography centered on the role of the state in accessing private information. It is important to note that at the same time the US was debating the de-listing of cryptography from ITAR, the Communications Assistance for Law Enforcement Act was being pushed forward in the US congress, meanwhile the National Security Agency in coordination with other law-enforcement agencies were pushing the introduction of the “Clipper Chip” to provide a secure backdoor into all US digital communications [43]. Additional constraints on the developing network and its legitimacy arose from its addressing architecture which centralized control into the hands of one person, Jon Postel. Such control was later exercised by the International Corporation for Assigned Named and Numbers (ICANN) under the National Telecommunications and Information Administration within the Department of Commerce [44].

As expanding Internet infrastructure increasingly made possible robust decentralized communication, the fight over who would control this communication was just getting started. Early utopian norm entrepreneurs such as Grateful Dead lyricist, John Perry Barlow, saw the fight as intimately related to rights [45]. As the conventional human rights community was regaining its footing after the 1980s and dealing with large geopolitical changes related to the collapse of the Soviet Union, concerns pertaining to the protection of rights in online spaces largely fell to the wayside. Yet some NGOs did arise and fought to include digital considerations in broader discussions of human rights.

Two prominent US based organizations, the Electronic Privacy Information Center (EPIC) (1994) and the Electronic Frontier Foundation (EFF) (1990), were established to defend civil liberties in the digital world. Concurrent to these formal norm entrepreneurs pushing forward or combating various forms of legislation, informal norm entrepreneurs in many countries built increasingly robust groups of hackers that challenged the status quo of what it meant to have rights in digital spaces. Groups including the Chaos Computer Club (1981) [46], Cult of the Dead Cow (1984) [47], L0ft (1992), and numerous others, expanded global interest into digital rights through cultural events, hacktivism and collective organization. Early language on digital rights sought to draw direct relationships between rights in online spaces and physical spaces.

Whereas the formation of rights leading up to and including the UDHR took several hundred years, early digital rights activists tried, and in many cases, succeeded in tying rights in one space to rights in the other. The passionate community of hackers combined with legal and policy wonks to foster robust dialogues on topics ranging from the vulnerabilities in government backdoors [48], to fundamental concerns pertaining to privacy [49]. These efforts have generated a range of governmental and non-governmental responses. Efforts such as the Internet Governance Forum and Multiple United Nations Governmental Groups of Experts, attempts by the International Telecommunications Union and others, have sought to raise to international attention critical issues pertaining to digital spaces. These efforts have spawned contentious debates on the role of state and non-state actors in the governance of the Internet [50, 51]. They have raised issues of multi-lateral versus multi-stakeholder involvement in how the Internet functions and what rights and privileges of individuals are to be protected and by whom. Internet governance debates do not lack norm entrepreneurs seeking to shape the identity of networks and netizens.

Although organizations including EPIC, EFF, Access Now, European Digital Rights, Digital Rights Watch, Internet Freedom Foundation, Fight for the Future, and several others, have increasingly sought to tie global Internet governance concerns to individual issues, these issues are often drowned out in technocratic and bureaucratic discussions. In particular, the technocratic push towards a future "utopia" of digital artefacts often undermines basic human rights normatively established and largely agreed to outside of digital spaces. Technocratic and market incentives are driving a divergence away from normative advances in human rights outside of digital spaces and resulting in a regression of digital human rights.

The next section examines the regression of human rights in digital space through both technical and policy lens and examines why norms of rights so robustly established outside of digital spaces are under so much threat within them.

4. Losing Utopia: The Regression of Digital Human Rights

A once quasi-anarchic, libertarian leaning space filled with hackers and NGOs fighting for "independence," free flows of information [52] linking societies around the globe in a generative [53] and collective march towards a better vision of efficiency and connectivity [54] is now increasingly contested. The norm entrepreneurs fighting for digital rights as human rights have not gone away. If anything, the number and scale of norm entrepreneurs fighting for digital rights has increased globally. Organizations traditionally focusing on human rights, democracy, and the rule of law in physical spaces, such as the National Democratic Institute, the International Republic Institute, and many others increasingly added to their portfolio digital rights. In the early 2000s under then Secretary of State, Hillary Clinton, digital rights defenders even found common cause with parts of the US government [55]. This common cause did not last long. In mid-2013 former NSA contractor Edward Snowden began releasing large volumes of documents through a variety of media outlets demonstrating the reach and extent to which the US government was capable of undermining digital rights online [56, 57].

How was utopia lost? First, it is important to note that the vision of utopia expressed by many academics, policymakers, and corporations did not exist in the way it was often portrayed. Notable pushback arose during this same period with some scholars applying a severely critical lens to the utopian visions being professed [58]. Moreover, there was substantial early analysis that suggested unease within much of the non-democratic world over the influx of new connected communications technologies [7]. Rebecca MacKinnon's efforts to document the multitude of violations arising from the influx of digital technologies illustrates that the present often regressive state of digital freedoms arose from a continually contested understanding of rights in digital spaces. Substantial evidence presented by Philip Howard and Muzammil Hussain underpinned the reality that states have been engaged in substantially repressive behaviour since networks started expanding outward in the late 1990s and into the early 2000s [59, 60]. In particular, Howard and Hussain write of the process through which new technologies were introduced into states and then subsequently repressed:

> A preparation phase, involving activists' use of digital media across time to build solidarity networks and identification of collective identities and goals; an ignition phase, involving symbolically powerful moments which ruling elites and regimes intentionally or lazily ignored, but which galvanized the public; a protest phase, where, by employing offline networks and digital technologies, small groups strategically organized on large numbers; an international buy-in phase, where digital media networks extended the range of local coverage to international broadcast networks; a climax phase, where the regime maneuvered strategically or carelessly to appease public discontent through welfare packages or harsh repressive actions; and finally, a follow-on information warfare phase, where various actors, state-based and from international civic advocacy networks, compete to shape the future of civil society and information infrastructure that made it possible [59].

The preparation, ignition, protest, international buy-in, climax, follow-on information warfare chain is in many ways an expanded understanding of norm dynamics presented by Finnemore and Sikkink in their work on international norm dynamics [2]. Early norm entrepreneurship for digital rights emphasized the spread of information communications technologies to countries along with the value such networks would bring with them [61]. Early internet freedom advocates saw the value of networks as tools for advancing human rights, many also recognized the subsequent repressive activities of states in response. The value of the networks in advancing technologies spawned multiple use case specific technologies to facilitate democracy and human rights. Projects such as the Guardian Project, the Tor Project, Tails, Cryptocat, and many others, provided a means for democracy and human rights activists to protect their data from intrusive states. These applications built on rapid developments in the open-source software and cryptography communities to enable network development in the later stages of the cycle proposed by Howard and Hussain when states increasingly used repression. Yet the reality remains, as demonstrated by the Snowden releases and reports of increasingly powerful malware developed by state and private corporate firms, that the ability to ensure human rights in networked spaces were increasingly under sustained threat [62–64].

Norm entrepreneurs for human rights in digital spaces have faced an ever-increasing array of challenges since 2010. Where once state-based actors were the principal threat to digital rights, the threat landscape has become increasingly complex as the technological landscape has shifted towards big data, machine learning, artificial intelligence [65], the Internet of Things (IoT) [66], and social networks [67–69]. At the forefront of the shifting vocabulary of norms on rights in digital spaces have been large technology companies [15]. The shift in vocabulary has positioned violations of human

rights as consequences of technological advances or temporary setbacks resulting from flaws in code or algorithmic design. Yet the systematic and pervasive penetration of technology into every facet of daily life in nearly every country around the world comes with profound consequences for the development of human rights in digital spaces. Disaggregating the attributes of the regression of human rights norms in digital spaces is complex as many technologies that have facilitated regression overlap and foster human rights challenges in divergent forms in different societies. In much the same way as conventional human rights violations occur and are addressed differently in different states, the same holds true for digital human rights violations.

As stated in the introduction, this paper cannot address all possible digital human rights violations, so instead it seeks to address those attributes that undermine human autonomy, empathy and dignity. Changing norms in digital spaces erode concepts of human autonomy, empathy, and dignity and therefore strike at the heart of normative discourses on digital human rights, they also serve as the fuel for digital rights regression. The regression of concepts pertaining to autonomy, empathy, and dignity arise from advances in data collection and data usage. Data collection can be further subdivided into either direct or passive interaction, while data usage can be subdivided into algorithmic (ML/AI) applications, hybrid, and individually targeted applications.

Data collection is no longer relegated to interactions of individuals in perceived digital space. Most users perceive digital interactions as originating from direct engagement with digital artifacts such as web-browsers, search engines, or other forms of active engagement. While early interactions in digital spaces were principally the result of direct interaction, the move from Web 1.0 to Web 2.0 and beyond has increasingly shifted the vast quantity of data interactions from active to passive engagements [70–72]. Examples of passive data collection abound. Presently individuals carrying mobile phones are constantly providing geolocation data with or without GPS settings activated. As individuals move between cell towers their relative position is relayed to the mobile provider. This relative position is tied to a device that in many countries is also tied directly to an individual's identity. The physical movement of the device in proximity to a person can provide data on whether an individual was in the vicinity of a perpetrated crime [73] or can be used to identify individuals engaged in protest [11].

Mobile devices are frequently used as navigational aids to assist drivers or other travellers as they move between destinations. These devices in turn provide substantial data on everything from user interests when stopping at stores or gas stations, to speed and telemetry data used at the individual level to monitor driving behaviour, or in aggregate to assess traffic patterns [74]. Passive collection data extends from the devices carried to individual level telemetry data in stores and public spaces through to use of Bluetooth protocols [75]. Individual level tracking mechanisms such as these are meant to provide greater efficiency to users and customers. They improve business efficiency and help facilitate the sale of advertisements. Yet in the process of providing data through constant passive interactions the individual loses autonomy. What at first glance appears to be pure gains in efficiency in turn is the conditioning of individuals through repeated passive interactions to shape and orient behaviour. Traffic guidance applications present notifications portraying advertisements to nearby shops, reroute traffic to avoid congestion through neighbourhood streets, and provide insurance companies with data to adjust automotive insurance rates [76]. While the above examples principally originate in the private sector, the technologies used are universal and governments around the world have increasingly relied on telemetry data derived from passive collection to facilitate state-based repression [77].

Violations of privacy are directly related to passive data collection and autonomy of self. Autonomy Privacy is defined as "an individual's ability to conduct activities without concern of or actual observation"[7]. Twenty to thirty years ago passively

[7] See: https://ethics.berkeley.edu/privacy/pisi

divulging information of a sensitive and personal nature to individuals would likely have been considered a substantial violation of privacy. Yet with the advent of tools capable of enabling passive data collection on individuals in nearly every aspect of their lives autonomy privacy has been eroded [78]. The intrusion of the digital world by both corporate and state actors is in direct violation of Article 12 of the UDHR:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks[8].

Yet in the span of 20 years what was once a human right has become a privilege, this is so because to secure the human right to privacy one must exclude oneself from modern social and economic infrastructures. Even a full exclusion of oneself from platforms and devices is not a guarantee of privacy. Social Media firms such as Facebook have found ways to collect data on individuals who do not even subscribe to their platforms [79]. In China new efforts to establish national facial recognition has resulted in the mass passive collection of data for state and corporate uses. The subsequent utilization of these data is virtually limitless [80]. Following in China's footsteps, India has begun the process of collecting and developing a national biometric database on its entire population [81]. Passive and active data collection are only likely to increase, this will result in further gross violations of privacy.

Data collection in online platforms is used both within and beyond digital spaces to undermine an array of human rights. Notable examples arise in China, which leverages big data to assess when online movements veer towards collective actions which might challenge the state or undermine state narratives [82]. The use of data collected from both passive and active engagements undermines the original utopian visions of the Internet as a platform for overcoming collective action problems [83]. Passive data collection even extends into private educational spaces as schools and universities have increasingly leveraged passive data collection to create models that can be used in later AI and ML applications to accuse students of cheating on digitally administered tests [84]. As private and state capacity to control data increases the autonomy of individuals and groups declines. This undermines several articles articulated under the UDHR, most notably articles 19 and 20[9]. Some norm entrepreneurs have had success in pushing back against the "more data is better" argument of business and many governments.

The General Data Protection Regulation which came into effect in 2018 is the principal example of a success which contrasts trends seeking to further erode rights in online spaces [85]. Implementation of the GDPR has had cascading impacts outside of European Union jurisdiction. Most easily recognizable of the impacts is the notification requiring users to accept the collection of cookies when visiting websites that might have users from the European Union. But just as this is an example of success, it is also an example of the embedded problems associated with safeguarding digital rights. The notification to accept cookies, instead of being a protective measure, is instead a further mechanism normalizing the collection of data through "user consent" [86, 87]. Just as most users fail to read the terms and conditions for most products and services due to their length and linguistically obtuse language, so too do users accept tracking cookies on web platforms. Although the GDPR has provisions safeguarding the rights of individuals in a digital environment the implementation of these rules is complex and requires constant oversight. Violations are punished principally through monetary fines.

Moving beyond discussion of data collection, the algorithmic manipulation of data erodes autonomy, undermines empathy, and imperils dignity. Just as most users are unaware that data is constantly being collected through passive interactions, they are also largely unaware of the impact that algorithms have on individual decisions.

[8] https://www.un.org/en/about-us/universal-declaration-of-human-rights

[9] Article 19 states: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." Article 20 states: "1. Everyone has the right to freedom of peaceful assembly and association. 2. No one may be compelled to belong to an association."

The manipulation of human decisions using algorithms occurs in the background, it is obscured via user interfaces and claims that these algorithms save time or simplify decision making processes. One of the most blatant examples of a private organization using algorithms for behavioural manipulation arose when Facebook undertook an experiment in which they presented only negative content in more than 700,000 user feeds [88]. The intent of the experiment was to generate an "emotional contagion" and by all accounts their experiment was a success. As a result of altering the algorithm Facebook was able to shift the emotional disposition of users. This power has profound human rights implications that are not well articulated within the existing UDHR. Facebook acknowledged in internal reports that the ability to successfully manipulate users could potentially alter democratic elections [89]. Such algorithmic manipulations demonstrably alter the notion of individual autonomy. Worse still, the use of algorithmic manipulation falls outside of the typical target of human rights obligation - governments - and instead empowers private actors to violate human autonomy as a result of market factors.

Issues of autonomy highlighted by the Facebook emotional contagion study are not the only area of concern. Manipulation of the psychological state of users, in particular levels of empathy, have been demonstrated to have mixed effects dependent on the structure and formulation of the information environments [90]. Network structures, as conditioned by algorithmic design, can in some instances impact the susceptibility of individuals to certain types of information that might either increase or decrease empathy towards issues and persons outside of one's own experience. Networks with algorithms fostering filter bubbles can alter the disposition of individuals in both positive (rights affirming) and negative (rights denying) manners [91]. The presentation of algorithms as neutral in curating the digital artefacts or in providing information to users is far from the truth. While software (of which algorithms of ML and AI are a subcategory) has often been perceived as agnostic politically, culturally, racially, and economically, it is in fact an expression of power intentionally or unintentionally constructed. Computer code, the instructions on which digital systems run, is the base construction of algorithms that make social media platforms, applications, and search engines function, it is a technical design with imbedded social and cultural values [92]. These values are not neutral. As a result the implementation of ML and AI not only reduces human autonomy but alters the empathy of users in ways that change their perception of rights and their perception of others.

Where Hunt illustrates how literature and art foster common humanity, Safiya Noble demonstrates that algorithms can have the opposite effect and result in the dehumanization of individuals [93]. Her work unequivocally demonstrates how platforms such as Google's search engine undermine the empathy critical to fostering and forming human rights claims within populations. Her work illustrates how platforms ostensibly developed to connect and share information can concurrently marginalize and undermine the political, social, and cultural positions of minorities and underprivileged groups. Expanding beyond bias embedded in the representation of individuals, algorithms have violated the equal right work considerations contained in Article 23 of the UDHR. Amazon and other companies used algorithms in their hiring systems to build profiles on potential employees. The result of these practices was substantial bias and reinforcement of existing labour pool ethnic composition [94]. The role of algorithms in undermining human rights even extends to the borders of nations and includes infringements on everything from privacy to freedom of movement [95].

Algorithms are increasingly pervading every aspect of modern digitally connected life. The implications for human rights violations arising from the development and use of algorithms is substantial and demonstrated [96]. Despite repeated documented failures and examples of algorithms resulting in human rights violations they, like big data collection, largely fall outside the purview of conventional human rights discourses. This is slowly changing as scholars address the legal and regulatory

consequences of their implementation in everyday life [97]. Increasingly discussions on the security of individual rights are being combined with concepts of cybersecurity and related topics and themes [98]. However, despite early efforts to reign in algorithms there remains a robust push to advance AI and ML applications without regard to their impact on digital human rights. Often this push is a function of market mechanisms embedded within surveillance capitalism, but just as frequently these use cases arise from academic scholarship at the nexus of computer science and multiple other fields of inquiry utilizing data and algorithms to solve specific problems. The challenge presented is almost the reverse of that faced by early norm entrepreneurs seeking to foster new conceptualizations of rights. With advances in data and algorithms it is the primacy of technological advance for some hypothesized utopian vision of an efficient and profitable world that overwhelms the rights-based discourse and fosters normative regression.

At the intersection of data and algorithms resides the central challenge to digital human rights. It is at this intersection where the dignity of human beings is undermined, where they are converted from UDHR Article 1 - "human beings born free and equal in dignity and rights" to potential manufacturers of data and consumers of products to be manipulated and directed in systems of digital control. It is here where the humanity of the human being is transferred into bits and bytes to be analyzed, organized, and directed. Data and algorithms are combining to enable technologies that undermine human dignity. Firms such as Cambridge Analytica prey on citizens in multiple countries around the world[10] through their data, and leverage algorithms to enable tailored manipulations to alter the outcomes of elections [69]. Firms manipulate the perceptions of human worth and value through the weaponization of information infrastructure for profit or political gain [99–101]. The constant and increasing challenges associated with data and algorithms impacting on human dignity are likely to grow as they influence everything from employment and education [102], to healthcare [103, 104] and criminal justice [105].

Big data collection and algorithms are fostering a steady regression in discourses on human rights in digital spaces. Rather than any one technology being presented as a fundamental violation of human rights, the issue at hand is a change in the normative discourse associated with rights secured in and through digital environments. Just as the march towards a common human rights discourse was slow and contested, the movement away from human rights in digital spaces is occurring in a slow, steady progress of technological advances, each attacking a slightly different area of concern. The failure to solidify the discourse around rights in digital spaces means that such rights have been exposed to the pressures of the market and the power of technological advance.

5. Re-establishing Digital Rights Norms

Kieron O'Hara and Wendy Hall present a compelling case that the regression of rights does not occur uniformly in all digital environments [106]. They argue that the political structures within nations in which networks grow and develop heavily influence how those networks are run and the rights associated with those networks [106]. They note that there are five "Internets" emerging globally. Among these are the Silicon Valley model of openness, the Brussels Bourgeois Internet, the DC Commercial Internet, The Beijing Paternal Internet, and the Moscow Spoiler Internet. Each of the five visions of the Internet in their analysis presents a unique set of policy and regulatory challenges. The argument that the Internet is fragmenting into zones of control and regulation is not new and has received some pushback from scholars such as Milton Mueller [107]. Different states are exerting different levels of control over their domestic Internets. Some states are increasingly repressive, while others are balancing the ills of openness with those of control. Yet what these arguments overlook is the advancing march of technology, in particular its ability to collect and use data in novel ways that strike at the heart of human rights discourses. The future of the Internet is uncertain. It is filled with enormous promise and peril. It is facing a future of information liberation [108] and censorship [109].

[10] See for example the discussion on the use of data by Cambridge Analytica to undermine Kenyan elections [118].

The evolution of human rights norms from shifts in autonomy, empathy, and the eventual definition of human dignity were not straightforward. While some individuals, landed white Christian males, experienced improvements in human rights earlier in the norm life cycle, the eventual development of the UDHR and a bevy of other conventions and laws at the national level shifted discourses and have made an impact. While early discourses on rights in digital spaces were strong and heavily supported by certain states, the consistent push for digital rights to be recognized and considered as human rights has suffered as technological advances have increasingly manipulated the conversation away from rights towards conversations on economics, efficiency, scientific advance and more. These counter norms and discourses damage the norms meant to foster autonomy, empathy, and dignity. They obscure their motives and impact with code and hardware. They shift the once quasi-utopian vision of a liberating Internet towards one that constrains rights and freedoms. Whereas the movement towards expanded human rights fought to elucidate and clarify those attributes of humanity that needed protection and from whom humans needed protection, the regression of rights in digital spaces is subtle and opaque. The march of technologies without thoughts to human security and rights approximates to the placing of a frog in a pot of water and slowly raising the temperature until it is boiled.

Digital technologies increasingly impact human autonomy, dignity, and empathy. They alter the way citizens, governments, and firms see and interact within one other. Technologies create dependencies and efficiencies that can and often do harm human security through reductions of human autonomy and the alteration of human empathy. Digital technologies create new means of violating human rights which are exclusively digital, they also extend older violation typologies from physical spaces to virtual ones. Yet of equal importance digital technologies can and do extend from virtual spaces back into physical spaces in ways that profoundly undermine human rights. In many ways digital rights violations are extremely pernicious because they extend into the personal spaces of individuals which were once free from surveillance mechanisms accessible to governments, firms, or even fellow. Rights once explicitly protected, are increasingly subject to terms of service, algorithmic design, pre-digital understandings of previously secured rights, and more. The result is that human autonomy in digital spaces is increasingly not a right, but a privilege secured through either payment to firms, or complex security practices learned and implemented by individuals. Through algorithms, networks, data collection and analysis, and platforms that shift the perceptions of others technologies are increasingly attacking the foundations of empathy that enabled recognition of autonomy within others. The combined result of the degradation of both human autonomy and empathy through digital means is the undermining of human dignity. As human dignity is undermined, human rights violations increase. This results in norms that regress away from expanded concepts of human dignity.

The regression of norms in digital spaces is remarkably progressed. Technical infrastructures are well on their way towards norm cascades if not already progressing towards internalization in discrete areas of data collection and usage. Science fiction is replete with the post norm cascade and internalization phases of the current regression of rights in digital spaces. One only need read Orwell's *1984, Ray Bradbury's Fahrenheit 451, Aldous Huxley's A Brave New World or more modern works by Cory Doctrow to gain a glimpse into the future where digital rights are consumed by advances in technologies. Ron Deibert is prescient in stating that a "Reset" is needed* [14]. Shoshana Zuboff's work serves as a canary in the proverbial coal mine warning that the world we are developing is not entirely as it seems [15]. There is a need to elevate a discourse of human rights in digital spaces. A solution has arisen in part in the European Union through the GDPR, but the networked nature of the Internet and the competing interests of states and their domestic Internets often forces rights considerations from the forefront to mere afterthoughts. It is unlikely that there will ever be a utopia predicated on rights-based discourses and norms, but neither should there be a dystopia.

REFERENCES

[1] A. Wendt, "Anarchy is what states make of it," *International Organization*, vol. 46, no. 2, 1992.

[2] M. Finnemore, K. Sikkink, "International norm dynamics and political change," *International Organization*, vol. 52, no. 4, pp. 887–917, 2003, doi: 10.1162/002081898550789.

[3] D. Ronald, *Access contested: Security, identity, and resistance in Asian cyberspace information revolution and global politics*. Cambridge, MA: MIT Press, 2012.

[4] R. Deibert, J. Palfrey, R. Rohozinski, J. Zittrain, *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA: MIT Press, 2010.

[5] R. Deibert, J. Palfrey, R. Rohozinski, J. Zittrain, *Access denied: The practice and policy of global internet filtering*. Cambridge, MA: MIT Press, 2008.

[6] A. Brantly, "The Cyber Losers," *Democracy and Security*, vol. 10, no. 2, pp. 132–155, 2014, doi: 10.1080/17419166.2014.890520.

[7] R. MacKinnon, *Consent of the networked: The worldwide struggle for Internet freedom*. New York, NY: Basic Books, 2012.

[8] L. Diamond, "Liberation Technology," *Journal of Democracy*, vol. 21, no. 3, pp. 69–83, 2010, doi: 10.1353/jod.0.0190.

[9] T. Zeynep, *Twitter and tear gas: The power and fragility of networked protest*. New Haven, CT: Yale University Press, 2017.

[10] A. Brantly, "From cyberspace to independence square: Understanding the impact of social media on physical protest mobilization during Ukraine's Euromaidan revolution," *Journal of Information Technology Politics*, pp. 1–19, 2019, doi: 10.1080/19331681.2019.1657047.

[11] A. Brantly. (2014, Jan. 24). *You were identified as a participant in a mass disturbance*. [Online]. Available: https://www.nditech.org/you-were-identified-participant-mass-disturbance. [Accessed: Nov. 29, 2022].

[12] B. Marczak, J. Scott-Railton. (2016, May 29). *Keep calm and (don't) enable macros: A new threat actor targets uae dissidents - the citizen lab*. [Online]. Available: https://citizenlab.ca/2016/05/stealth-falcon/. [Accessed: Nov. 29, 2022].

[13] J. Scott-Railton, S. Hardy. (2014, Dec. 18). *Malware attacks targeting syrian isis critics*. [Online]. Available: http://citizenlab.ca/2014/12/malware-attack-targeting-syrian-isis-critics/. [Accessed: Nov. 29, 2022].

[14] R. Deibert, *Reset: Reclaiming the Internet for civil society*. Toronto, ON: Anansi, 2020.

[15] S. Zuboff, *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, New York: PublicAffairs Press, 2019.

[16] H. Lynn, *Inventing human rights: A history*. New York: W.W. Norton & Company, 2007.

[17] R. Dean, *The value of humanity in Kant's moral theory*. New York: Oxford University Press, 2006.

[18] D. von der Pfordten, "On the dignity of man in Kant," *Philosophy*, vol. 84, no. 3, pp. 371–391, 2009, doi: 10.1017/s0031819109000370.

[19] M. Wollstonecraft, *A vindication of the rights of woman. Harmondsworth*. UK: Penguin Books, 1975.

[20] C. Beccaria, G. Newman, P. Marongiu, *On crimes and punishments*. New Brunswick, NJ: Transaction Publishers, 2009, doi: 10.4324/9781315125527.

[21] Voltaire, S. Harvey, *Treatise on tolerance*. Cambridge, UK: Cambridge University Press, 2000.

[22] E. Weitz, *A world divided: the global struggle for human rights in the age of nation-states*. Princeton, NJ: Princeton University Press, 2019.

[23] H. Arendt, *The origins of totalitarianism*. New York: Harcourt Brace, 1985.

[24] J. Kingdon, *Agendas, alternatives, and public policies*. New York: Longman, 2003.

[25] J. Donnelly, *Universal human rights in theory and practice*, 3rd ed. Ithaca, NY: Cornell University Press, 2013.

[26] United Nations, *Universal declaration of human rights*. [Online]. Available: https://www.un.org/en/about-us/universal-declaration-of-human-rights. [Accessed: Mar. 9, 2022].

[27] J. Habermas, "The concept of human dignity and the realistic utopia of human rights," *Metaphilosophy*, vol. 41, no. 4, 2010.

[28] A. Moravcsik, "Explaining international human rights regimes: Liberal theory and Western Europe," *European Journal of International Relations*, vol. 1, no. 2, pp. 157–189, 1995.

[29] T. Solomon, "Norms and human rights in international relations," *Political Studies Review*, vol. 4, no. 1, pp. 36–47, 2005, doi: 10.1111/j.1478-9299.2006.00038.x.

[30] M. Caprioli, P. F. Trumbore, "Human rights rogues in interstate disputes, 1980–2001," *Journal of Peace Research*, vol. 43, no. 2, pp. 131–148, 2006, doi: 10.1177/0022343306061356.

[31] E. Neumayer, "Do international human rights treaties improve respect for human rights?," *Journal of Conflict Resolution*, vol. 49, no. 6, pp. 925–953, 2005, doi: 10.1177/0022002705281667.

[32] K. Sikkink, "Human rights, principled issue-networks, and sovereignty in Latin America," *International Organization*, vol. 47, no. 3, pp. 411–441, 1993, doi: 10.1017/s0020818300028010.

[33] B. Simmons, *Mobilizing for human rights: international law in domestic politics*. Cambridge, UK: Cambridge University Press, 2009.

[34] J. Abbate, *Inventing the Internet*. Cambridge, MA: MIT Press, 2000.

[35] K. Hafner, M. Lyon, *Where wizards stay up late: The origins of the Internet*. Simon & Schuster, 1996.

[36] P. Baran. (1962). *On distributed communications networks*. [Online]. Available: https://pages.cs.wisc.edu/~akella/CS740/F08/740-Papers/Bar64.pdf. [Accessed: Nov. 29, 2022].

[37] F. Heart. (1970). *Interface message processors for the ARPA computer network*. [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD0709621.pdf. [Accessed: Nov. 29, 2022].

[38] V. G. Cerf, R. E. Kahn, "A protocol for packet network intercommunication," *Data Communications of the IEEE Communications Society*, p. 1–13, 1974.

[39] L. DeNardis, *Protocol politics: the globalization of Internet governance*. Cambridge, MA: MIT Press, 2009.

[40] A. Brantly, "A holistic approach to the encryption debate," in *Cyber insecurity: navigating the perils of the next information age*, T. Herr, R. Harrison, Eds. Lanham, Maryland: Rowman & Littlefield, 2016.

[41] D. Kehl, A. Wilson, K. Bankston. (2015). *Doomed to repeat history? Lessons from the Crypto Wars of the 1990s*, Open Technology Institute. [Online]. Available: https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf. [Accessed: Nov. 29, 2022].

[42] A. F. Brantly, "Conceptualizing cyber policy through complexity theory," *Journal of Cyber Policy*, pp. 1–15, 2019, doi: 10.1080/23738871.2019.1583763.

[43] S. K. Pell, "You can't always get what you want: How will law enforcement get what it needs in a Post-CALEA, cybersecurity-centric encryption era?," *North Carolina Journal of Law and Technology*, vol. 17, no. 4, pp. 599–643, 2016.

[44] H. Klein, "ICANN and internet governance: leveraging technical coordination to realize global public policy," *Information Soc*, vol. 18, no. 3, pp. 193–207, 2011, doi: 10.1080/01972240290074959.

[45] J. P. Barlow. (1996). *A declaration of the independence of cyberspace*, Electronic Frontier Foundation. [Online]. Available: https://www.eff.org/cyberspace-independence. [Accessed: Aug. 30, 2021].

[46] M. Webb, C. Doctorow. (2020). *Coding democracy: how hackers are disrupting power, surveillance, and authoritarianism*. [Online]. Available: https://img1.od-cdn.com/ImageType-100/0111-1/{024C8725-D290-45E4-944F-0057B65CFB00}Img100.jpg. [Accessed: Nov. 29, 2022].

[47] J. Menn, *Cult of the Dead Cow: How the original hacking supergroup might just save the world*. New York: PublicAffairs, 2019.

[48] H. Abelson, R. Anderson. S.M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P.G. Neumann, R.L. Rivest, J.I. Schiller, B. Schneier, M. Specter, D.J. Weitzner, "Keys under doormats: mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity*, vol. 44, no. 1, p. tyv009–11, 2015, doi: 10.1093/cybsec/tyv009.

[49] W. Diffie, S. Landau, *Privacy on the line, updated and expanded edition*. Cambridge, MA: MIT Press, 2007.

[50] M. L. Mueller, *Networks and states: The global politics of internet governance*. Cambridge, MA: MIT Press, 2013.

[51] L. Denardis, *The global war for Internet governance*. New Haven, CT: Yale University Press, 2014.

[52] A. Greenberg, *This machine kills secrets: How WikiLeakers, cypherpunks and hacktivists aim to free the world's information*. New York: Dutton, 2012.

[53] J. Zittrain, *The future of the Internet and how to stop it*. New Haven, London: Yale University Press, 2008.

[54] C. Shirky, *Here comes everybody: The power of organizing without organizations*. New York: Penguin Press, 2008.

[55] H. R. Clinton. (2011, Feb. 15). *Remarks on Internet freedom*. [Online]. Available: https://www.eff.org/files/filenode/clinton_internet_rights_wrongs_20110215.pdf. [Accessed: Nov. 29, 2022].

[56] BBC News. (2014, Jan. 17). *Edward Snowden: Leaks that exposed US spy*. [Online]. Available: http://www.bbc.com/news/world-us-canada-23123964. [Accessed: Nov. 29, 2022].

[57] G. Greenwald. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. [Online]. Available: http://www.glenngreenwald.net/. [Accessed: Nov. 29, 2022].

[58] E. Morozov, *The net delusion: The dark side of internet freedom*. New York: Public Affairs, 2011.

[59] P. N. Howard, S. D. Agarwal, M. M. Hussain, "When do states disconnect their digital networks? Regime responses to the political uses of social media," *The Communication Review*, vol. 14, no. 3, pp. 216–232, 2011, doi: 10.1080/10714421.2011.597254.

[60] M. M. Hussain, P. N. Howard, "What best explains successful protest cascades? ICTs and the fuzzy causes of the arab spring," *International Studies Review*, vol. 15, no. 1, pp. 48–66, 2013, doi: 10.1111/misr.12020.

[61] Y. Benkler, *The wealth of networks: how social production transforms markets and freedom*. New Haven, CT: Yale University Press, 2006.

[62] J. Scott-Railton, B. Marczak, S. Anstis, B. A. Razzak, M. Crete-Nishihata, R. Deibert. (2018). *RECKLESS VI: Mexican journalists investigating cartels targeted with nso spyware following assassination of colleague*, The Citizen Lab. [Online]. Available: https://tspace.library.utoronto.ca/bitstream/1807/96737/1/Report%23116--Reckless%20VI.pdf. [Accessed: Nov. 29, 2022].

[63] B. Marczak, A. Abdulemam, N. Al-Jizawi, S. A. Berdan, J. Scott-Railton, R. Deibert. (2021, Aug. 24). *From Pearl to Pegasus Bahraini government hacks activists with NSO Group Zero-Click iPhone exploits*, The Citizen Lab. [Online]. Available: https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphoneexploits/. [Accessed: Aug. 30, 2022].

[64] K. Zetter. (2021, July 22). *The NSO 'surveillance list': What it is and isn't*, Zero Day. [Online]. Available: https://zetter.substack.com/p/the-nso-surveillance-list-what-it [Accessed: Aug. 30, 2022].

[65] P. Tucker, *The naked future: What happens in a world that anticipates your every move*. New York: Current, 2014.

[66] S. J. Shackelford, *Internet of things*. New York: Oxford University Press, 2020.

[67] J. Lukito, "Coordinating a multi-platform disinformation campaign: Internet research agency activity on three US social media platforms, 2015 to 2017," *Political Communication*, vol. 37, no. 2, pp. 1–18, 2019, doi:10.1080/10584609.2019.1661889.

[68] P. N. Howard, M. M. Hussain, "The role of digital media," *Journal of Democracy*, vol. 22, no. 3, pp. 35–48, 2011, doi: 10.1353/jod.2011.0041.

[69] K. C. Desouza, A. Ahmad, H. Naseer, M. Sharma, "Weaponizing information systems for political disruption: The actor, lever, effects, and response taxonomy (ALERT)," *Computers and Security*, vol. 88, p. 101606, 2019, doi: 10.1016/j.cose.2019.101606.

[70] T. Lehtiniemi, "Personal data spaces: An intervention in surveillance capitalism?" *Surveillance & Society*, vol. 15, no. 5, pp. 626–639, 2017, doi: 10.24908/ss.v15i5.6424.

[71] M. Zajc, "The social media dispositive and monetization of user-generated content," *Information Society*, vol. 31, no. 1, pp. 61–67, 2014, doi: 10.1080/01972243.2015.977636.

[72] S. Brewster et al., "Social media as a passive sensor in longitudinal studies of human behavior and wellbeing," CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1–8, 2019, doi: 10.1145/3290607.3299065.

[73] A. Bogomolov, B. Lepri, J. Staiano, N. Oliver, F. Pianesi, A. Pentland, "Once upon a crime: Towards crime prediction from demographics and mobile data," *Arxiv*, 2014, doi: 10.48550/arXiv.1409.2983.

[74] R. Bolla, F. Davoli, "Road traffic estimation from location tracking data in the mobile cellular network," vol. 3, pp. 1107–1112, 2000, doi: 10.1109/wcnc.2000.904783.

[75] D. Oosterlinck, D. F. Benoit, P. Baecke, N. V. de Weghe, "Bluetooth tracking of humans in an indoor environment: An application to shopping mall visits," *Applied Geography*, vol. 78, pp. 55–65, 2017, doi: 10.1016/j.apgeog.2016.11.005.

[76] S. Abdelhamid, H. S. Hassanein, G. Takahara, "Vehicle as a mobile sensor," *Procedia Computer Science*, vol. 34, pp. 286–295, 2014, doi: 10.1016/j.procs.2014.07.025.

[77] S. Feldstein, *The rise of digital repression: How technology is reshaping power, politics, and resistance*. New York: Oxford University Press, 2021.

[78] T. M. Payton, T. Claypoole, *Privacy in the age of big data: recognizing threats, defending your rights, and protecting your family*. Lanham, MD: Rowman & Littlefield, 2014.

[79] A. Hern. (2018, Apr. 17). *Facebook admits tracking users and non-users off-site*, The Guardian. [Online]. Available: https://www.theguardian.com/technology/2018/apr/17/facebook-admits-tracking-users-and-non-users-off-site. [Accessed: Mar. 14, 2022].

[80] X. Qiang, "The road to digital unfreedom: President Xi's surveillance state," *Journal of Democracy*, vol. 30, no. 1, pp. 53–67, 2019, doi: 10.1353/jod.2019.0004.

[81] C. Pope, "Biometric data collection in an unprotected world exploring the need for federal legislation," *Journal of Law and Policy*, vol. 26, no. 2, pp. 769–803, 2018.

[82] G. King, J. Pan, M. E. Roberts, "How censorship in China allows government criticism but silences collective expression," *American Political Science Review*, vol. 107, no. May, p. 326–343, 2012, doi: 10.1017/s0003055413000014.

[83] S. González-Bailón, J. Borge-Holthoefer, A. Rivero, Y. Moreno, "The Dynamics of Protest Recruitment through an online network," *Scientific Reports*, vol. 1, no. 1, p. 197, 2011, doi: 10.1038/srep00197.

[84] K. Hylton, Y. Levy, L. P. Dringus, "Utilizing webcam-based proctoring to deter misconduct in online exams," *Computers & Education*, vol. 92, pp. 53–63, 2016, doi: 10.1016/j.compedu.2015.10.002.

[85] G. A. Teixeira, M. M. da Silva, R. Pereira, "The critical success factors of GDPR implementation: a systematic literature review," *Digital Policy Regulation and Governance*, vol. 21, no. 4, pp. 402–418, 2019, doi: 10.1108/dprg-01-2019-0007.

[86] W. L. Youmans, J. C. York, "Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements," *Journal of Communication*, vol. 62, no. 2, pp. 315–329, 2012, doi: 10.1111/j.1460-2466.2012.01636.x.

[87] E. P. Robinson, Y. Zhu, "Beyond 'I agree': Users' understanding of web site terms of service," *Social Media + Society*, vol. 6, no. 1, 2020, doi: 10.1177/2056305119897321.

[88] D. Hunter, N. Evans, "Facebook emotional contagion experiment controversy," *Research Ethics*, vol. 12, no. 1, pp. 2–3, 2016, doi: 10.1177/1747016115626341.

[89] P. Gerbaudo, F. Marogna, C. Alzetta, "When 'positive posting' attracts voters: User engagement and emotions in the 2017 UK election campaign on facebook," *Social Media + Society*, vol. 5, no. 4, 2019, doi: 10.1177/2056305119881695.

[90] A. G. Shu-Sha, H. Sophia, C. Jennifer, R. Andrea, "Social media use and empathy: A mini meta-analysis," *Social Networking*, vol. 8, no. 4, pp. 147–157, 2019, doi: 10.4236/sn.2019.84010.

[91] L. V. Bryant, "The youtube algorithm and the alt-right filter bubble," *Open Information Science*, vol. 4, no. 1, pp. 85–90, 2020, doi: 10.1515/opis-2020-0007.

[92] A. J. Flanagin, C. Flanagin, J. Flanagin, "Technical code and the social construction of the internet," *New Media & Society*, vol. 12, no. 2, pp. 179–196, 2010, doi: 10.1177/1461444809341391.

[93] S. U. Noble, "Algorithms of oppression: How search engines reinforce racism", *NYU Press*, pp. 119–133, 2018, doi: 10.2307/j.ctt1pwt9w5.8.

[94] M. Hildebrandt et al., "Mitigating bias in algorithmic hiring," Proceedings of the 2020 Conference on Fairness, Accountability and Transparency, pp. 469–481, 2020, doi: 10.1145/3351095.3372828.

[95] M. Oluwasanmi, "Algorithms and the border: The human rights implications of automated decision systems in Canadian immigration," *Federalism-E*, vol. 22, no. 1, 2021.

[96] J. Gerards, "The fundamental rights challenges of algorithms," *Netherlands Quarterly of Human Rights*, vol. 37, no. 3, pp. 205–209, 2019, doi: 10.1177/0924051919861773.

[97] L. McGregor, D. Murray, V. Ng, "International human rights law as a framework for algorithmic accountability," *International and Comparative Law Quarterly*, vol. 68, no. 2, pp. 309–343, 2019, doi: 10.1017/s0020589319000046.

[98] J. S. Hiller, G. Berger-Walliser, A. F. Brantly, "Critical protection for the network of persons," *Journal of Law and Social Change*, vol. 25, no. 2, pp. 117–152, 2021.

[99] C. W. Fitzgerald, A. F. Brantly, "Subverting reality: The role of propaganda in 21st century intelligence," *International Journal of Intelligence and Counterintelligence*, vol. 30, no. 2, pp. 215–240, 2017, doi: 10.1080/08850607.2017.1263528.

[100] G. Bolsover, P. Howard, "Computational propaganda and political big data: Moving toward a more critical research agenda," *Big Data*, vol. 5, no. 4, pp. 273–276, 2017, doi: 10.1089/big.2017.29024.cpr.

[101] P. N. Howard, S. Woolley, R. Calo, "Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration," *Journal of Information Technology and Politics*, vol. 15, no. 2, pp. 1–13, 2018, doi: 10.1080/19331681.2018.1448735.

[102] R. S. Baker, A. Hawn, "Algorithmic bias in education," *International Journal of Artificial Intelligence in Education*, 2021, doi: 10.1007/s40593-021-00285-9.

[103] T. Panch, H. Mattie, R. Atun, "Artificial intelligence and algorithmic bias: Implications for health systems," *Journal of Global Health*, vol. 9, no. 2, 2019, doi: 10.7189/jogh.09.020318.

[104] A. Brantly, N. D. Brantly, "Patient-centric cybersecurity," *Journal of Cyber Policy*, vol. 5, no. 3, pp. 1–20, 2020, doi: 10.1080/23738871.2020.1856902.

[105] A. Završnik, "Algorithmic justice: Algorithms and big data in criminal justice settings," *European Journal of Criminology*, vol. 18, no. 5, pp. 623–642, 2021, doi: 10.1177/1477370819876762.

[106] K. O'Hara and W. Hall, *Four internets: Data, geopolitics, and the governance of cyberspace*. New York: Oxford University Press, 2021.

[107] M. Milton, *Will the Internet fragment?: Sovereignty, globalization and cyberspace*. Cambridge: Polity Press, 2017.

[108] C. Baxter, O. Tkacheva, M. C. Libicki, L. H. Schwartz, J. E. Taylor, J. Martini, *Internet freedom and political space*. Santa Monica, CA: The RAND Corporation, 2013.

[109] M. E. Roberts, *Censored: Distraction and diversion inside China's great firewall*. Princeton, NJ: Princeton University Press, 2018.

[110] V. Carty, *Social movements and new technology*. New York and London: Routledge, 2015.

[111] M. Joyce, Ed., *Digital activism decoded: The new mechanics of change*. New York: International Debate Education Association, 2010.

[112] B. Rolfe, "Building an electronic repertoire of contention," *Social Movement Studies*, vol. 4, no. 1, pp. 65–74, 2005, doi: 10.1080/14742830500051945.

[113] R. Rohrschneider, R. Dalton, "A global network? Transnational cooperation among environmental groups," *The Journal of Politics*, vol. 64, no. 2, pp. 510–533, 2002.

[114] S. H. Kamel, "Egypt's ongoing uprising and the role of social media: Is there development?" *Information Technology for Development*, vol. 20, no. 1, p. 78–91, 2014, doi: 10.1080/02681102.2013.840948.

[115] A. Karatzogianni, *Cyber conflict and global politics*. Abingdon, Oxon: Routledge, 2009, doi: 10.4324/9780203890769.

[116] V. P. Shannon, "Norms are what states make of them: The political psychology of norm violation," *International Studies Quarterly*, vol. 44, pp. 293–316, 2000.

[117] S. Moyn, *Not enough human rights in an unequal world*. Cambridge, MA: Harvard University Press, 2018.

[118] N. Nanjala, *Digital democracy, analogue politics: How the internet era is transforming Kenya*. London, UK: Zed Books LTD, 2018.