PRIVACY, HUMAN RIGHTS, AND WEB 3.0

Danyella Johnston, Gyu Myoung Lee, Sorren Hanvey, Áine MacDermott

Liverpool John Moores University, School of Computer Science and Mathematics

ABSTRACT

Technology and our networked environment has made privacy an increasingly challenging state to achieve but in order to ensure we continue to meet the foundational standard for human rights, it is essential that privacy is elevated as a priority global discussion. We must continually review whether technology and network deliverables are meeting a privacy standard in a format accessible to all. In this paper we review whether Web 2.0 has met the required standard and if not, what impact this has had on society. From this we ask what we need to address in Web 3.0 to ensure those inadequacies do not proliferate into Web 3.0 developments. Finally, this paper offers five human rights centric privacy design principles for future development.

Keywords – Web 2.0, data privacy, semantic web

1. INTRODUCTION

'When you say, "I don't care about the right to privacy because I have nothing to hide", that's no different to saying I don't care about freedom of speech because I have nothing to say, or freedom of the press because I have nothing to write.' Snowden [1]

The idea of defining privacy has existed since Aristotle [2] and the debate has considered the philosophical, sociological, political, moral, and legal implications of these definitions [3-5]. Whether privacy is seen as a *right* to determine what information about oneself is shared with others, or as a measure of *control* over what information is shared, or a *state* of limiting access of oneself to others [6, 7], the theme we see throughout is, as Thomson states, no-one actually 'seems to have any clear idea of what it is' [8]. Although in and of itself this statement was not directed toward *privacy* but instead the *right* to privacy [9]. Solove argued that because privacy is not one thing but instead a 'cluster of many distinct yet related things' [10] it serves little purpose to try to provide an all-encompassing definition, and as stated by Hartzog, it is futile to obsess over a 'singular and definitive conceptualization of privacy' [11]. However, in recent years it has become more important to debate the boundaries and definition of privacy in the context of how technology makes it an increasingly challenging state to achieve. Therefore, this paper will move away from the detail-oriented discussion regarding individualistic ideas of privacy and instead consider the broader risks presented by recent technological advances. It will consider privacy not from the general terms of the UNs Universal Declaration of Human Rights 1948 Article 12 (UDHR A12), or the European Convention on Human Rights 1953 Article 8 (ECHR A8) [12], but instead consider all articles within those declarations in terms of them being at risk through the advent of technology that may jeopardize general standards of privacy and our right to freedom of thought, identity, conscience, opinion, and expression, without fear of retribution. We will ask if technological advances in Web 2.0 (W2.0) have weakened privacy rights to a level that jeopardizes the framework needed for many other human rights to exist. We will do this by identifying where W2.0 privacy models have been manipulated or mismanaged and the resulting impact from those privacy deficient designs. Throughout, we will consider developments against a backdrop of the human rights identified within UDHR and ECHR as necessary for a healthy and prosperous society to thrive. We will also consider all recommendations against the UNESCO Guidelines for the Governance of Digital Platforms (GGDP) [13] and will ask if the lessons learned from the development of W2.0 can guide us in identifying potential privacy risks in Web 3.0 (W3.0) design strategies. Finally, we will propose a set of human-rights-centric privacy design principles that would underpin a Human Rights Data and Technology (HRDaT) framework.

2. PRIVACY AND HUMAN RIGHTS

Since Warren and Brandeis conceived the 'right to be let alone' [14] discussions have often skirted away from the challenges of conceptualizing privacy, instead attempting to contextualize it through legal frameworks and in later years technological design. From a rights definition perspective we see sweeping statements in declarations such as UDHR A12 whereby 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation' [15] and in ECHR A8. Although neither of these declarations make attempts to define what privacy is, or what arbitrary interference of privacy or respect for privacy entails, thus leaving both statements open to debate. Later the Human Rights Act 1998 Article 8 (HRA A8), whilst not expanding on the definition within the Act itself, does in part attempt to loosely define privacy in its supporting documentation. It refers to a private life 'without government interference' and talks of your right to 'determine your sexual orientation, your lifestyle, and the way you look and dress.' It goes on to link your private life

to the development of your personal identity, including your 'right to participate in essential economic, social, cultural and leisure activities' that underpin that identity [16].

Definitions of privacy are related to the concept of identity, and as such, are both fundamental to the establishment of human rights. Privacy is about autonomy over who collects and uses a person's private information, and identity is about autonomy over being regarded as a unique individual made up of many characteristics and historical events. The narrative view of personal identity focuses on our ability to engage in storytelling and to create narratives about ourselves and as such we need to be able to select or omit the information we share about ourselves as we require [17]. In the Convention on the Rights of the Child Article 16 we see the mirroring of UDHR A12 in regard to privacy, but it also specifically calls out protections for identity in Articles 8 and 29 [18]. Whilst privacy and identity are closely related and arguably feed one another, there are differences [19]. However, those differences do not detract from the argument that by infringing upon someone's privacy we also interfere with their identity. Unfortunately, we see the two concepts merge as data processors argue the need to verify an 'identity' to be able to participate in their service offering securely, and in doing so mine all characteristics of a person for the most mundane services. It is in the interest of data collectors to understand identity as that will indirectly influence our behaviors [20] but this is a commercially driven reason to validate identity rather than a security reason. For us to have moral agency, we need to have the ability, as Laceulle states, to 'live well, with and for others, according to one's deepest aspirations and best capacities, as full participating members of a society/community' [17]. If this engagement is only permitted through the relinquishment of our privacy, then we are not being allowed to participate in society or to realize our moral agency without threat of exclusion from that community should we wish to withhold information. This condition in and of itself removes the agency we need to secure our identities.

As with privacy and identity, privacy and anonymity are related yet distinct concepts. Anonymity, a fundamental requirement in modern democratic politics, is the absence of identifying traits or the concealment of them. Privacy on the other hand is the restriction of those identifiers from the public gaze [21]. Relating anonymity to privacy has become part of the discussion regarding civil rights and inclusivity, with the concealment of hierarchizing identity markers offering opportunities for meritocracy and to challenge the corporate and political power structures that jeopardize human rights. For this paper, we will not debate absence vs restriction and the potential associated challenges to accountability but will take the position that any future ecosystem should have the ability to restrict identifiers to a level of concealment appropriate to the functionality of the application being utilized. In a W3.0 ecosystem this could be supported by other technical design structures such as smart contracts and cryptographic hashing. For example, a voting solution requires full concealment, but the application could restrict voting on a one vote per Self Sovereign Identity (SSI) basis [22]. The voter is then concealed but the integrity of the process is maintained.

Over time focus has moved from general policy declarations to guiding frameworks such as the General Data Protection Regulation (GDPR) and UK Data Protection Act 2018 (DPA 2018), and Digital Personal Data Protection Act 2023 (India) which are among many rules introduced by governments aimed at protecting society from potential overreach by private and public sector entities. Unfortunately, these frameworks have in some cases been unable to limit the very governments who implemented them from overstepping consent mechanisms put in place to protect individuals and society. We should also note that despite policy efforts to empower online users regarding how they choose to share their data, online service providers privacy policies are shown to not provide real consumer options if users want to engage in services [23]. Without this control at an individual level, society remains exposed for wider risks to our democratic civil rights.

Identity, anonymity, and policy are seen here as structural elements of the privacy and human rights debate which are foundational to social structure and how individuals interact and communicate with one another. Therefore, how we design communication and social connection tools such as the web becomes a discussion on how those tools can and will influence society and human rights.

3. IMPACT OF THE WEB

The term Web 1.0 (W1.0) and later W2.0 are considered by Berners-Lee to be a misnomer that implies W2.0 was something apart from W1.0, but in fact the functionality was all based on W1.0 standards and has simply been a more fully realized version of the original vision. However, post the dot-com crash the team at O'Reilly had been looking to reassure the public that the Web was just as important as ever, and so coined the phrase W2.0, not to distinguish the next phase as a new set of technologies, but more a societal shift in financial interest and support [24]. That said, there is an acknowledged step change of capability in this phase of development, whether conceptually intended or not. It sees W1.0 in its static user content consumption form, morph into a social and collaborative user-generated content tool.

When considering the development of W2.0 the technical advances are almost overshadowed by the societal impact they have had. We saw commentators evangelizing about the potential societal benefits of the democratization of data and the redistribution of political power. Lev Grossman wrote in Time magazine (2006) 'It's a story about community and collaboration on a scale never seen before […]. It's about the many wrestling power from the few and helping one another for nothing and how that will not only change the world, but also change the way the world changes. The tool that makes this possible is […] Web 2.0, as if it were a new version of some old software. But it's really a revolution' [25]. At the heart of these references is the belief we were moving knowledge from the hands of the few into the hands of the

many, and in doing so humankind would change for the greater good. What many seemed to not appreciate was that the developers of these new ways of working were not driven by altruism but instead by the capitalist model which already existed within society. In 1996, Borsook wrote a scathing commentary for Mother Jones about the myopic regard Silicon Valley had toward regulation in the earlier years of technology development. They stated "Technolibertarians rightfully worry about Big Bad Government, yet think commerce unfettered can create all things bright and beautiful—and so they disregard the real invader of privacy: Corporate America seeking ever-better ways to exploit the Net, to sell databases of consumer purchases and preferences, to track potential customers however it can" [26]. In other words, we may have created new ways of doing things but the drivers for doing them never altered.

3.1 Surveillance capitalism

Surveillance capitalism is one of the many ways W2.0 privacy models failed us, and it has had wide implications. Our data is harvested through social platforms, retailers, healthcare providers, financial institutions, network services, government departments, and IoT devices within our homes and operational infrastructures. We do this for the promise of increased security, social connectivity, and simplified consumerism. However, we have witnessed obvious privacy erosion through extensive data collection and advertising models created on the back of it. It is forecast there will be more than 29.4 billion IoT connected devices worldwide by 2030 [27], Facebook collects 4 Petabytes of data per day and has more than 2.2 billion active users per month [28] and it is predicted there will be 6.4 billion people connected to the web through mobile devices by 2029 [29]. In turn Facebook generated $40.11 billion revenue in Q4 2023 [30] and the IoT market generated revenue of $970 billion worldwide in 2022 [31]. These revenues are driven at least in part by the data being accessed by these corporations, making data one of the most valuable commodities in the world. Our personal data equates to the monetization of human attention and these business models are now entrenched in global markets. The implementation of policy and governance alone is not enough to contain the demand of shareholders for more revenue, which requires more data. Therefore, for us to maintain our privacy and human rights, and to remove the commodity status assigned to us by corporations, we must ensure a new set of proactive privacy design principles to underpin the reactive governance policies in place.

3.2 Trust Implications

In 2023, 78% of people surveyed in the US stated that they trusted themselves to make correct decisions to protect their privacy and data, although 61% said they were skeptical their information would be treated responsibly [32]. This trend of distrust is mirrored by a 2023 Deloitte survey, which indicated 77% of smartphone users and 62% of smart home device users were concerned about privacy on their devices. The study noted users sense of futility at trying to stop the misuse of their data, with 27% believing companies would track them no matter the measures they put in place, and only half of respondents believing the benefits of services outweighed their privacy concerns [33]. This unease is not unfounded with stories of big tech overreach and behavioral manipulation regularly hitting the worlds press. Examples include Cambridge Analytica, who were accused of manipulating voter opinions in the 2016 US elections and 2016 UK Brexit vote via the illegal collection, analysis, and subsequent targeting of millions of Facebook accounts; the Facebook Emotional Manipulation Experiment (2012); and Project Alamo (2016). The American Psychological Association notes that a core element of identity is 'the feeling that one's memories, goals, values, expectations, and beliefs belong to the self [34]' but can we be sure our identities are our own whilst corporations manipulate what we see and how we respond? For human rights standards to be met, we must ensure that defense from psychological and ideological manipulation and abuse is central to how we develop technology privacy models for the future.

3.3 Governance Overreach and Censorship

Democratic governments have been shown to disregard concepts of individual rights with scandals such as the US NSA Prism program, the use of Pegasus Spyware by multiple governments, and the Indian governments use of the Aadhaar System. Human Rights Watch recently raised concerns regarding Indian authorities control over their digital ecosystem stating that the risk of technology misuse during the 2024 elections was considerable. They went on to call for technology companies to take additional steps to ensure the protection of human rights during India's elections [35]. This is in addition to the extensive data surveillance being levied on the citizens of many non-democratic and pseudo-democratic countries, with reports of facial recognition and mandatory data-sharing from tech companies to government bodies, as measures to control political dissent. Many of these forms of surveillance have only been exposed through activist intervention such as Wikileaks Vault 7, the Snowden Reports, and the Hacking Team leak, however privacy activist organizations have also challenged government attempts to access personal information such as the UK Investigatory Powers Act, Australia's Data Retention Law, and Turkeys Social Media Regulation, stating that they are simply legal pathways to go around privacy and associated human rights.

Voltaire was attributed with saying, "I disapprove of what you say, but I will defend to the death your right to say it." [36] This same foundational idea has built the US Bill of Rights Amendment 1 (freedom of speech and of the press), ECHR A10 (freedom of expression), and UDHR A18 (freedom of thought, conscience, and religion). Surveillance has far-reaching consequences regarding censorship, with links through history of censorship tactics being an indicator of emerging or established authoritarian states. It is not a new concept, with book burning and book bans established as a cornerstone of controlling knowledge and sending a message that non-conforming ideas and ideals would be met with similar heavy-handed tactics [37]. As we moved into the cyberspace, these controls have been implemented by corporations on behalf of governing states or sometimes

independent of them. Whilst this controls the content being seen rather than the private data of users wishing to see it, it is indicative of the profound impact on freedom of speech caused by the centralization of data and data access points. It also raises concerns for users worried that attempts to access this information are being monitored and logged.

3.4 Peer-surveillance and self-censorship

We have witnessed an exponential increase in deep fake development, AI developed revenge porn, and cyberstalking, and whilst the impacts can potentially be felt by everyone the greatest impact has been on women and minorities with studies showing more than 70% of cyber-stalking victims are women [38]. We see similar kinds of digital intimidation being used in attempts to silence environmental defenders, human rights organizations, and journalists [39]. These tactics have led to fears within human rights defense groups that policy and legal governance alone are not enough to protect the human rights of those who challenge commercial and political strategies. For the right to freedom of thought and political dissent without fear of retribution we must provide privacy solutions that support opportunities for discourse. With fear of retaliation and cancel culture there is also an understandable psychological imperative for citizens to censor themselves. There is a desire to avoid balanced and rational political, religious, or ideological commentary in an environment of algorithms that encourages extreme opinion due to its virality and potential monetization of human attention. This has extensive implications on societies ability to meet human rights on a global scale. One driver behind self-censorship is a perceived lack of adequate legal protections. A separate debate, beyond the remit of this paper, must discuss the balance between privacy, censorship, and the greater good of society. For this paper however, we argue that embedded privacy would give greater voice to the moderates and minorities who currently avoid debate for fear of online or physical retaliation.

4. THE PRIVATE SPACE CREATED BY WEB 3.0

Partly in response to the open and decentralized W1.0 becoming an oligopoly of holding companies and tech giants that is now W2.0, and partly because the phoenix that was Berners-Lee's original vision was arguably always going to emerge from the ashes, we now have the advent of W3.0. Differences in how we consume information across the three iterations of the Web ecosystem can be seen in Figure 1. Hailed as the decentralized ecosystem that will allow users to regain controls over their privacy, and for innovation and competition to return to the markets [40], W3.0 has enormous potential. Only however, if we design it to be resistant to the sociological and economic models that created the W2.0 problems. Through blockchain technology and decentralization there is hope for more inclusivity, equitability, interconnected collaboration, and security in the digital world [41]. Shifting from centralized server architectures controlled by entities driven by short-term financial goals, into distributed networks with peer-to-peer protocols and user-centric models, we could become carried

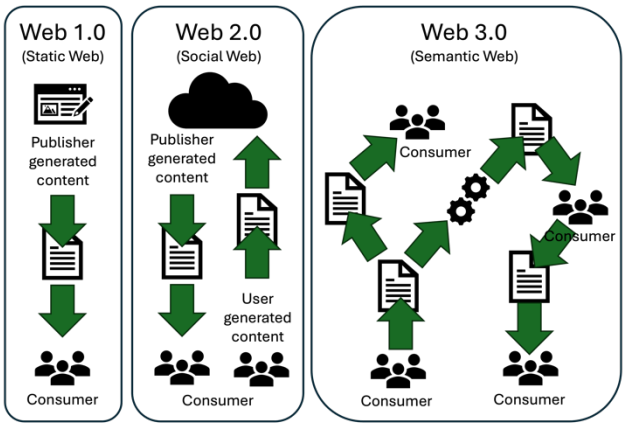

Figure 1. How content is consumed and generated

away by the dream. However, the dream can only be realized when the reality of collaboration, co-ordination, and governance is accepted, and the risk of poor strategic conceptualization has been accounted for.

From an economics standpoint, monopolies are shown to increase wealth gaps and poverty, whereas increased market competition increases innovation and the redistribution of wealth with associated positive societal shifts. Through its distributed ledger technology (DLT) across a node network ecosystem, blockchain is the foremost enabler of W3.0 decentralization, which provides opportunities to redistribute control from centralized agents. Underpinned by consensus algorithms, cryptographic hashing, and mostly open development protocols it offers transparent, immutable, and verifiable information across its network. The decentralizing character of blockchain reduces barriers to enter markets and scale at a competitive pace, thereby offering opportunities to redistribute influence into online communities that can develop across physical and economic landscapes. This has the potential to reduce the centralized entity benefits behind surveillance capitalism business models. However, although the transparency and transaction traceability of the DLT model allows the decentralized node network to exist, there needs to be adequate protections to reduce opportunities for tracing pseudo-anonymous addresses against other data sources that allow for data aggregation and identity profiling. Other issues include the concept of data immortality, caused by data addition to the blockchain being near impossible to change or delete, meaning if data is exposed it is arguably exposed forever; scalability and energy consumption issues with privacy concepts such as zero-knowledge proofs which slow down the network; and the current lack of fluid interoperability which is required for an effective SSI solution to be developed. However, by addressing these challenges in future development, the decentralized nature of this design, supported by SSI, allows the strongest response to the W2.0 surveillance problems, by reducing opportunities for centralized agents to aggregate personal data.

4.1 Self-sovereign identity (SSI)

Self-sovereign identity (SSI) is the concept of removing intermediaries from the identity management chain through decentralization, thereby removing centralized repository

architectures from the data identification design flow. This is done by giving individuals tools such as digital wallets to manage who has access to their data for verification and transaction services via their personal devices. SSI design flow uses claims (requests), proofs (evidence), and attestations (validation) allowing individuals to choose what they share and when. As well as the increase to personal privacy this model reduces risk derived from attacks to large scale centralized data stores. Through this design individuals create unique decentralized identifiers (DIDs) to create public keys for verification allowing secure peer-to-peer connections. This is supported by authentication, service endpoints, timestamps, and private key signatures to ensure verifiable histories. As well as offering opportunities for removing intermediaries from the verification process for individuals, SSI can be used by legal entities to verify their DID with company documents. One main challenge to SSI is its lack of interoperability, although developments such as OpenAPI Specification and Open Telemetry standards are working towards addressing this. Once challenges are addressed however, SSI alongside the blockchain becomes integral to removing centralized surveillance models.

4.2 Decentralized Autonomous Organizations (DAO)

DAO's are models built on blockchains utilizing W3.0 technologies, digital assets, and democratic decision-making processes to distribute resources and coordinate activities. They constitute technical frameworks that allow governance and consensus decision making by eligible participants, which leads to collaborative user stakeholder engagement and drives collective benefits rather than individualistic corporate benefits. The privacy element of this model allows for distributed funding without identity bias, thereby improving the human rights of groups who may otherwise be marginalized by centralized organizations. As DAOs are underpinned by automated smart contract parameters, it is essential that contracts are designed with privacy-preserving mechanisms that only require essential data points to execute the steps needed to complete the contract. Whilst DAOs allow transactions and governance without the need for an intermediary to collect and store personal data, privacy remains paramount in a model that requires transaction transparency to reinforce the token-based voting model.

4.3 Data Cooperatives (DC)

Where DAOs focus on removing third party intermediaries, DCs are working on negotiating the terms of service against which intermediaries can remunerate members for access to data pools. They are membership-based organizations specifically focused on managing data as a collective source. They are not inherently tied to the blockchain, with distributed database, federated cloud service, encryption, data trust frameworks, and API management all offering potential avenues to create a DC. However, blockchain self-sovereign protections have the potential to simplify and increase trust to such concepts. Whilst DCs allow users to monetize their data and often work on a one-member one-vote decision making basis, challenges arise if a member becomes unhappy with group decisions impacting their data.

4.4 Censorship resistance

Decentralization, immutability, transparency, and peer-to-peer networking creates an environment resistant to censorship. Coupled with privacy models such as SSI this allows for everyone to participate equally in the conversation about local, state, and global policy without fear of retribution. However, we must be cognoscente that although the blockchain itself is censorship resistant, the application layer could still introduce control points or vulnerabilities that potentially allow censorship. Therefore, it is essential we introduce technology design principles that discourage development that may allow for this, whilst championing designs that introduce real self-sovereign privacy controls. Other challenges that have been raised include concerns over anonymity being an opportunity for increased illicit and/or society damaging activities. A study of Tor entry nodes estimated that around 6.7% network users accessed 'Onion/Hidden Services' that are disproportionally used for illicit activities [42]. However, one problem with using Tor based indicators in discussions regarding the impact of increased web privacy, is that Tor users are already a sub-set of technically competent web users looking for increased privacy to avoid corporate and government oversight. Therefore, it could be argued that the percentage of those doing so for negative social benefits is higher than those who currently do not seek Tor protections and are interacting with the web in the knowledge that they may be being surveilled.

4.5 Security vulnerabilities

There are several potential security vulnerabilities for the blockchain such as 51% attacks, poorly written smart contracts, Sybil attacks, routing attacks, time-jacking, and endpoint vulnerabilities, although the impact to personal data is minimized by its structure. Whilst a single individual may suffer loss of data through a smart contract vulnerability or end-point security breach, the effort and cost to complete these kinds of attacks on a mass scale for the purpose of accessing data becomes a deterrent to malicious agents. That does not remove the risk altogether, as we are aware of the proliferation of social engineering phishing scams but the ability to access large data sets with a similar impact to historical W2.0 breaches is made near impossible. By moving the data loss risk from a centralized control point to individual users through SSI, we increase protections against malicious agents who would acquire mass datasets, mine the data for vulnerability markers, and make use of that information for more targeted attacks on individuals. This increased protection frees users to be more open in expressing their identities without concerns about whether a central agent is appropriately protecting that information.

4.6 Regulatory and watchdog oversight

If we change our communication and trade structure from centralized institutions acting as gatekeepers, to peer-to-peer trading, what do we do if something goes wrong and our data is breached? To avoid the centralized controls of the current W2.0 model we must avoid creating brokers and agents that

sit between W3.0 interactions. However, without governance structures that help standardize controls and measure accountability against a set of design principles and expectations, how do we ensure quality control across development? Is developer consensus enough to ensure standards are met? It could be argued volunteer developer consensus has been successfully trialed in W2.0 with open-source systems being widely adopted and maintained. A recent example however, demonstrated the risks around open source when a 'supply chain' hack against Linux distributions saw a back door access point introduced by a 'volunteer developer'. The vulnerability was identified by another developer before it was rolled out across the public domain but it highlighted the risks associated with reliance on the good will of a few dedicated technicians [43].

4.7 Migration of Web 2.0 to Web 3.0

One key consideration is how W3.0 will connect to W2.0 applications to ensure continuity of services to users. If we consider the impact moving to an SSI privacy model on W3.0 will have for tech giants and government agencies, it is easy to conclude there will not only be push back but a race to try to develop the same privacy models in W3.0 as we currently have in W2.0. Users may also find themselves in positions whereby they have to opt out of certain community relationships or services because those providers refuse to transition or bridge to the new SSI model. The risk to our overarching human rights as we push for SSI has the potential to be vast and should not be underestimated simply because the current abuses are also great.

5. HRDAT

This paper proposes that to ensure the human rights aligned ideology and integrity of W3.0, there needs to be an overarching Human Rights Data and Technology framework (HRDaT) that provides a privacy-focused design strategy. Figure 2 offers a process flow representing key modules and stakeholders that need to be accounted for in the HRDaT. For this framework to be designed the first step is to identify more specific and actionable technology privacy principles for developers as they relate to human rights, than is currently offered by the UNESCO GGDP. Whilst the GGDP has made great strides in associating technology development to human rights and provides an excellent source of guidance for UN States to understand their duties in supporting those rights from a technology perspective, the principles for developers are more generally associated to content curation and moderation than focused on privacy. It is essential that we refocus attention to privacy if these governing bodies wish to embed human rights into technology design. As we have seen in this paper, content moderation is not a driver for freedom of expression and identity. Only by embedding privacy through decentralizing W3.0 technologies can we hope to guarantee those rights. Foundational to the HRDaT this paper offers five human rights and privacy focused technology design principles created to align to UDHR, ECHR, HRA, and GGDP.

5.1 Respect for human dignity

Technology development should prioritize and respect human dignity in all its forms through the adequate protection of individuals identities. The data collected, algorithms developed, and the platforms designed should not allow for the degradation, dehumanization or discrimination of individuals or groups, whether those individuals participate in the service provided or not. *Example: Data collected should only be for the minimum data points required to validate the security of a service. Collection beyond this requirement has historically been used for surveillance, profiling, or decisions that have led to discrimination, therefore additional data points should be fully transparent and optional for individuals.*

5.2 Transparency and accountability

Technology developers must be transparent about how their technologies work and why they require the data points they request in a way that is considered informed consent. For communication to be transparent developers must ensure information regarding services is accessible to all regardless of education level, age, cognitive ability, language, disability, or any other distinction. *Example: Clear communication regarding the collection of data and the use of algorithms should be provided to individuals before the service is engaged with and should be in a language that is accessible to the user, and accounts for age, cognitive variations, and potential disabilities.*

5.3 Right to challenge

Technology providers will be held accountable via redress and remediation frameworks, for any impact they have on individuals and society through the misuse or loss of private data. These frameworks will be designed to ensure that any perpetuation of existing inequalities through the collection, manipulation, profiling, and/or mishandling of private data has a clear pathway for redress and remediation. Providers will also be required to report on an open forum, the amount and type of data processed and the purposes it has processed that data for. *Example: Existing frameworks such as GDPR and governing bodies such as the Information Commissioners Office (ICO) may be given stronger powers to govern and enforce punitive damages as well as fines. An open forum for data processors to report annually the types and amount of data being processed alongside the revenue generated from e.g. marketing, could assist in transparency and oversight efforts.*

5.4 Minimum standards of privacy

Technology developers must consider the collection of data beyond the minimum data points required to validate the security of a service, as a privilege and not a right. All platforms must prioritize individual users as their primary stakeholders considering their right to privacy as the number one driver within any business model. This is not limited to security but also includes how the data is processed, for what purposes, who is the beneficiary of any processing outputs, and how the data is stored. *Example: Technology providers should ask whether the data being collected is for the well-being and service of the user, or for the financial interests of the company or its investors whether directly or indirectly. Whilst a company*

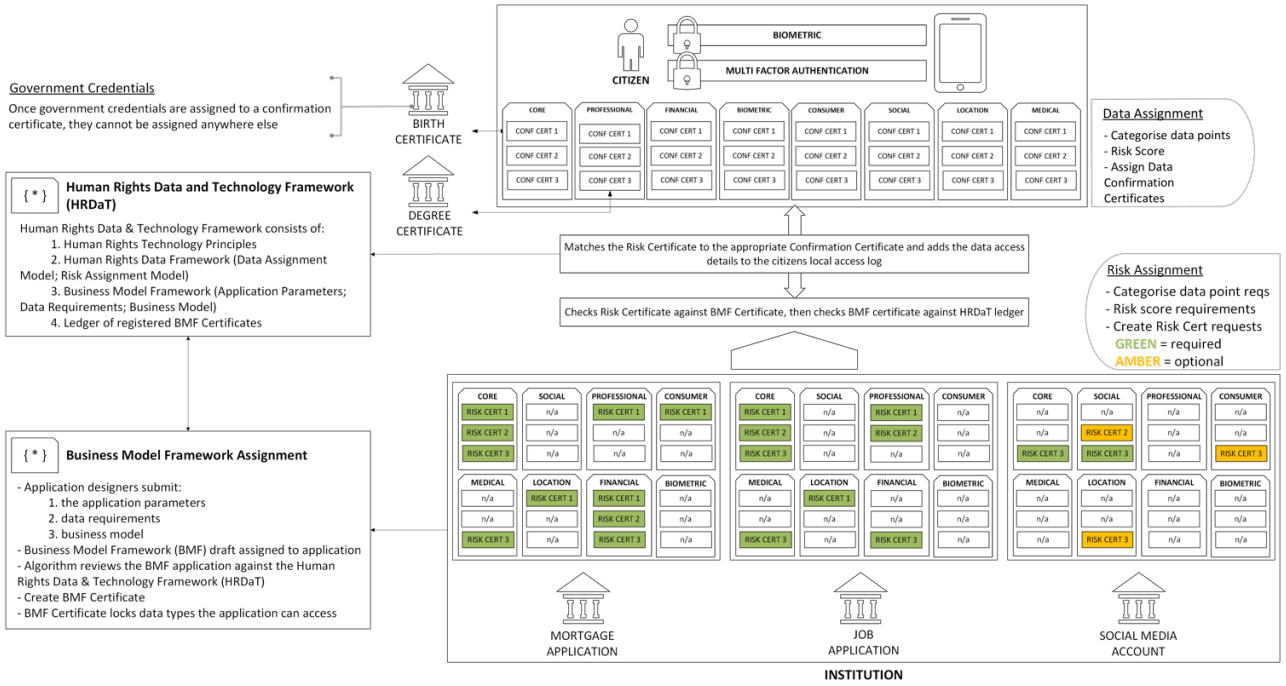

Figure 2. Human Rights Data and Technology Framework

needs to remain viable, it should not be at the detriment of the privacy and security of individuals or groups of individuals.

5.5 Decentralization

Technology designs should support an ecosystem of decentralized self-sovereignty that recognizes no borders whether digital or physical. The decentralized design principle should allow greater freedom of movement and opportunities for individuals to remove themselves from environments which do not meet our expectations for human rights. *Example: Decentralization and SSI reduce opportunities for surveillance by agents who would hold individuals in a state of servitude or slavery, and/or restrict freedom of movement, and/or inhumanely treat individuals or groups. Through SSI individuals also hold more control over data which may be used to attack their reputation or to discredit them during democratic challenges to politically biased policies.*

6. CONCLUSION

In this paper we have argued that privacy underpins our ability as a society to meet the human rights standards set out in UDHR and ECHR. It has made the case that current W2.0 privacy models not only undermine but actively remove many of the human rights of minority and politically non-conforming groups through the centralization of personal data and data access points. It went on to review the opportunities and risks associated with moving from a centralized W2.0 to a decentralized W3.0 ecosystem, highlighting where questions remain outstanding. It has shown that for us to be able to re-establish our human rights in a digital future, we require the decentralization offered by W3.0 as it allows for a self-sovereign ecosystem that can support privacy based human rights. Finally, this paper has offered a set of five human rights-based privacy driven technology principles as the foundation of an overarching HRDaT framework, aimed at refocusing developers towards a single strategic pathway supporting global human rights. This paper recommends future research to validate the specific W3.0 technical designs required to achieve each of the five principles across varying industry sectors and business models. Also, for compliance and governance frameworks to be able to hold technology providers accountable against these principles, new frameworks for measuring human rights centric impacts must be derived from multi-disciplinary research inviting input from political science, economics, psychology, sociology, philosophy, and law, to name a few. Additionally, research should look at how wider society, as the majority stakeholder in the discussion, is informed and educated on emerging changes to technology and the impacts that has on their human rights. Providing non-technical citizens with tools to protect their human rights holds little value if those stakeholders do not understand how to use them effectively or the impact their decisions are having on their human rights or the accumulative rights of their social networks.

REFERENCES

[1] A. Rusbridger, E. MacAskill, and J. Gibson, ed., "Edward Snowden: a right to privacy is the same as freedom of speech – video interview," theguardian.com, 2015.

[2] J. Swanson, The Public and Private in Aristotle's political Philosophy, Cornell University Press, London, 1992.

[3] F. Schoeman, “Privacy: Philosophical Dimensions,” American Philosophical Quarterly, vol.21, no.3, pp. 199-213, 1984.

[4] K. Nissim, A. Wood, “Is privacy privacy?,” Philosophical Transactions: A Mathematical, Physical and Engineering Sciences, vol.376, no.2128, pp. 1-17, 2018.

[5] W. L. Prosser, “Privacy,” California Law Review, vol.48, no.3, pp. 383-423, 1960.

[6] R. Gavison, “Privacy and the Limits of Law,” The Yale Law Journal, vol.89, no.3, pp. 421-471, 1980.

[7] L. Menges, “Three Control Views on Privacy,” Social Theory and Practice, vol.48, no.4, pp. 691-711, 2022.

[8] J. Thomson, “The Right to Privacy,” Philosophy & Public Affairs, vol.4, no.4, pp. 295-314, 1975.

[9] K. O’Hara, The seven veils of privacy: How our debates about privacy conceal its nature, Manchester University Press, 2023.

[10] D. J. Solove, Understanding Privacy, Harvard University Press, Massachusetts & London, 2008.

[11] W. Hartzog, “What is Privacy? That's the Wrong Question,” The University of Chicago Law Review, vol.88, no.7, pp. 1677-1688, November 2021.

[12] "European Convention on Human Rights," 08/04/24; www.echr.coe.int/documents/d/echr/convention_ENG.

[13] UNESCO Guideline for the Governance of Digital Platforms, UNESCO, 2023.

[14] S. Warren, L. Brandeis, “The Right to Privacy,” Harvard Law Review, vol.4, no.5, pp. 193-220, 1890.

[15] "Universal Declaration of Human Rights," 08/04/24; www.un.org/en/about-us/universal-declaration-of-human-rights.

[16] "Human Rights Act 1998, Article 8," 13/04/24; www.equalityhumanrights.com/human-rights/human-rights-act/article-8-respect-your-private-and-family-life.

[17] H. Laceulle, "Narrative identity and moral agency," Aging and Self-Realization: Cultural Narratives about Later Life, Transcript Verlag, pp. 127-158, 2018.

[18] "Convention on the Rights of the Child," 15/04/24; www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

[19] C. Sullivan, "Digital Identity: Consequential Individual Rights," Digital Identity: An Emergent Legal Concept, University of Adelaide Press, pp. 71-106, 2011.

[20] K.-L. Alfrey, et.al., “The Role of Identity in Human Behavior Research: A Systematic Scoping Review,” Identity, vol.23, no.3, pp. 208-223, 2023.

[21] H. Asenbaum, “Anonymity and Democracy: Absence as Presence in the Public Sphere,” The American Political Science Review, vol.112, no.3, pp. 459-472, 2018.

[22] S. Cucko, et.al., “Towards the Classification of Self-Sovereign Identity Properties,” IEEE access, vol.10, pp. 88306-88329, 2022.

[23] C. Prince, et.al., “Are We Living in Surveillance Societies and Is Privacy an Illusion? An Empirical Study on Privacy Literacy and Privacy Concerns,” IEEE Transactions on Engineering Management, vol.70, no.10, pp. 3553-3570, 2023.

[24] A. E. Marwick, "A Cultural History of Web 2.0," Status Update: Celebrity, Publicity, and Branding in the Social Media Age, Yale University Press, pp. 21-72, 2013.

[25] L. Grossman. "You Yes, You Are TIME's Person of the Year," 09/04/24; https://content.time.com/time/magazine/article/0,9171,1570810,00.html

[26] P. Borsook, "Cyberselfish," Mother Jones, 1996.

[27] "Number of IOT Connected Devices Worldwide 2019-2023 With Forecasts to 2030," 24/04/24; www-statista-com.eu1.proxy.openathens.net/statistics/1183457/iot-connected-devices-worldwide/.

[28] M. Osman. "Wild and Interesting Facebook Statistics and Facts," 14/04/24; https://kinsta.com/blog/facebook-statistics/

[29] "Number of mobile internet users worldwide from 2020 to 2029," 24/04/24; www-statista-com.eu1.proxy.openathens.net/forecasts/1146312/mobile-internet-users-in-the-world.

[30] N. Buchanan. "What You Need To Know Ahead of Meta's Earnings Report," 24/04/24; www.investopedia.com/metaq1-fy-2024-earnings-preview-8630822#:~:text=Analysts%20project%20Meta's%20revenue,estimates%20compiled%20by%20Visible%20Alpha.

[31] Internet of Things: market data & analysis, Statista, 2023.

[32] C. McClain, et.al., How Americans View Data Privacy, Pew Research Center, 2023.

[33] J. Arbanas, et.al., "Data Privacy and Security Worries are on the Rise, While Trust is Down," 24/04/24; www2.deloitte.com/xe/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/data-privacy-and-security.html.

[34] "Identity," 20/03, 2024; https://dictionary.apa.org/identity.

[35] Human Rights Watch. "India: Technology Use Shouldn't Undermine Free, Fair Elections," 04/05/24; www.hrw.org/news/2024 /04 /08/india-technology-use-shouldnt-undermine-free-fair-elect ions.

[36] E. B. Hall, (Tallentyre, S.G). "The Friends of Voltaire," 05/05/24; www.gutenberg.org/cache/epub/56618/pg56618-images.html.

[37] L. Boissoneault. "A Brief History of Book Burning, From the Printing Press to Internet," 05/05/24; www.smithsonianmag.com/history/brief-history-book-burning-printing-press-internet-archives-180964697/.

[38] R. Cahal, et.al., “Cyber Stalking: Technological Form of Sexual Harassment,” International Journal on Emerging Technologies, vol.10, no.4, pp. 367-373, 2019.

[39] F. Sammut, M. Bezzina, J. Scerri, “Under Attack in the Cyber Battlefield: A Scoping Review of Journalists’ Experiences of Cyberharassment,” Journalism Practice, pp. 1-29, 2023.

[40] A. Murray, K. Dennie, J. Combs, “The promise of a decentralized internet: What is Web3 and how can firms prepare?,” Business horizons, vol.66, no.2, pp. 191-202, 2023.

[41] P. P. Ray, “Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions,” Internet of Things and Cyber-Physical Systems, vol.3, pp. 213-248, 2023.

[42] E. Jardine, A. M. Lindner, G. Owenson, “The potential harms of the Tor anonymity network clusters disproportionately in free countries,” Proceedings of the National Academy of Sciences - PNAS, vol.117, no.50, pp. 31716-31721, 2020.

[43] A. Hern. "How one man stopped a potentially massive cyber-attack, by accident," 05/05/23; www.theguardian.com/global/2024/apr/02/techscape-linux-cyber-attack.