UNIVERSITY OF PENNSYLVANIA
JOURNAL OF LAW AND SOCIAL CHANGE
Volume 27, Number 1 **Draft** 2023

Internet Human Rights

Michael J. Kelly & David Satola[†]

Abstract

The rate at which Internet connectivity is spreading is matched only by the increasing amount of time people spend online. Today over 5 billion humans access the Internet; the overwhelming majority of them engage in social media, and almost all of them live out key aspects of their daily lives digitally. Human rights are universal in the sense that they apply to everyone, everywhere. And while there are indicators that they apply in cyberspace, how they apply is a different story.

Now, as the Universal Declaration of Human Rights (UDHR) turns 75, we wonder how many of those rights accompany us into our digital lives. This article develops a matrix mapping how human rights developed for the physical world might apply in the digital world, using the 30 articles (rights) enumerated in the UDHR as a foil. As a result, the broad outline of a clearer picture emerges, whereby some governments or courts mandate certain rights to fully manifest in digital space, while others are making progress, and still others remain static. Moreover, enforcement can occur via either state regulation or corporate terms of service.

Designed as the first tool of its kind for attorneys, judges, policymakers, and advocates to chart which rights are accompanying us onto and into the Internet, this guide will be a foundational starting point for a much broader discussion to come.

[†] Michael Kelly holds the Sen. Allen A. Sekt Endowed Chair in Law at Creighton University School of Law; David Satola is Lead Counsel, Technology and Innovation at the World Bank. Together, Professor Kelly and Mr. Satola Co-Chair the American Bar Association's Task Force on Internet Governance for the Business Law Section's Cyberspace Law Committee. The authors are grateful for research assistance by Sapphire Anderson, Christena Rogers, and Corey Lamas. The views expressed herein are those of the authors and do not necessarily reflect those of the World Bank or the American Bar Association.

"Remember when, on the Internet, nobody knew who you were?"

Introduction

In a 1994 interview with Rolling Stone, Apple founder Steve Jobs observed, "Technology is nothing. What's important is that you have a faith in people, that they're basically good and smart, and if you give them tools, they'll do wonderful things with them."[1] By January 2023, "there were 5.16 billion Internet users worldwide, which is 64.4 percent of the global population."[2] The overwhelming number of those Internet users, 4.76 billion, were engaging with social media platforms.[3]

What these billions of people are doing on the Internet is as varied as they are. Hopefully, the faith placed in them by Steve Jobs to be doing wonderful things is not misplaced. Regardless, humanity's massive, persistent, and growing online presence is what drives us to reflect on where we spend most of our time in the modern world. As the below graph by the Pew Research

[1] Jeff Goodell, *Steve Jobs in 1994: The Rolling Stone Interview*, ROLLING STONE (Jan. 17, 2011), https://www.rollingstone.com/culture/culture-news/steve-jobs-in-1994-the-rolling-stone-interview-231132/ [https://perma.cc/F7US-72WD].

[2] Ani Petrosyan, *Worldwide Digital Population 2023*, STATISTA (APR. 3, 2023), https://www.statista.com/statistics/617136/digital-population-worldwide/ [https://perma.cc/V8TX-XY3Y].

[3] *Id.*

Center below indicates, over 80% of Americans are online daily and almost 30% are online constantly.[4]

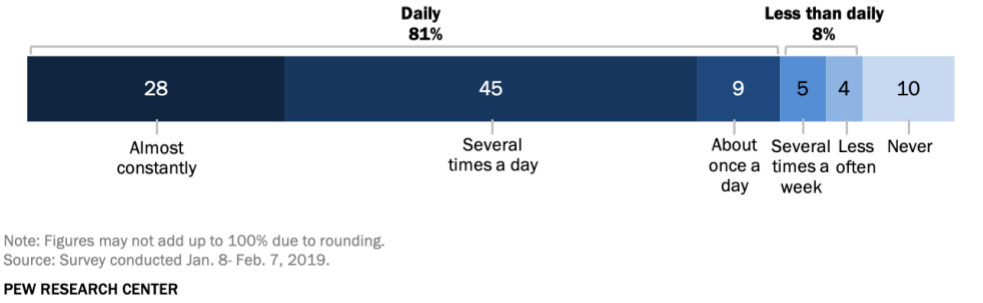

Figure 1: Frequency of Daily Internet Access in the United States.

As an interconnected global society, we find ourselves looming over the edge of a virtual precipice; on the other side awaits full digital reality. We've been peering into this world for decades with both awe and wonder. As the kinetic physical world in which we exist recedes and the digital world in which we increasingly live and work takes up more space in our lives, we must begin thinking about how that digital existence should evolve. In particular, how do human rights—designed and articulated in and for an analogue world—feature in our digital existence?

In December 2023, the United Nations will commemorate the 75th anniversary of the Universal Declaration of Human Rights.[5] As a legal framework, human rights embody our values and protect our freedoms as a species. The universality of their application is a foundational premise: by virtue of one's status as a *homo sapiens*, one is accorded a standard set of

[4] Andrew Perrin & Sara Atske, *About Three-in-Ten U.S. Adults Say They Are 'Almost Constantly' Online*, PEW RSCH. CTR. (Mar. 26, 2021), https://www.pewresearch.org/fact-tank/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/ [https://perma.cc/YP6B-8HZ8] ("Adults under the age of 50 are at the vanguard of the constantly connected: 44% of 18- to 49-year-olds say they go online almost constantly. By comparison, just 22% of those ages 50 to 64 and even smaller shares of those 65 and older (8%) say they use the internet at this frequency.").

[5] *See* Kathryn McNeilly, *'If Only for a Day': The Universal Declaration of Human Rights, Anniversary Commemoration and International Human Rights Law*, 23 HUMAN RIGHTS L. REV. 1 (2023).

rights without question to race, gender, religion, or class. If this framework is to exist alongside us in digital space, how does that manifest itself? States are obligated to enforce international human rights law extraterritorially[6]—presumably this includes in cyberspace as well.

Some rights have already fully manifested and achieved complete enforceability. The most legally developed example is the transference of what we know in the physical realm as the "right to privacy" into what has become known in the digital realm as the "right to be forgotten."[7] This version of the right to privacy empowers citizens within the European Union to petition Google to redact information about them that Google returns to searchers as search results. Although resisted by Google as an improper deputization of a multinational corporation as an information censor,[8] and by the British press as an improper infringement of freedom of the press and an assault on free speech,[9] the European Court of Justice nevertheless determined that the individual privacy of rights of E.U. citizens could best be protected in this manner—thus bringing this human right into full digital reality.[10]

However, with respect to enforcement, Google prevailed in its resistance to France's Internet regulator, Commission Nationale de l'Informatique et des Libertés, which asserted that when granted, such right to be forgotten requests had to be taken down globally—the ECJ holding that such information only had to be redacted from search results in Europe.[11] Thus, searchers in India or Canada could still see full search results for a German or Italian individual that searchers in E.U. in countries such as Romania or Belgium could not see. This transference of offline human rights to online manifestation is known as the normative equivalency paradigm, wherein offline rights are simply taken online.[12]

Some scholars believe the change in such rights during transference fundamentally changes their nature and enforceability, and have challenged the utility of the normative equivalency paradigm, calling for a new paradigm

---

[6] Dafna Dror-Shpoliansky & Yuval Shany, *It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology*, 32 EUR. J. INT'L L. 1249, 1256 (2021) [hereinafter Dror-Shpoliansky & Shany].

[7] Michael J. Kelly & David Satola, *The Right to Be Forgotten*, 2017 U. ILL. L. REV. 1, 1 (2017) [hereinafter Kelly & Satola].

[8] *Id.* at 21.

[9] *Id.* at 35-36.

[10] *Id.* at 6–10.

[11] Leo Kelion, *Google Wins Landmark Right to Be Forgotten Case*, BBC (Sep. 24, 2019), https://www.bbc.com/news/technology-49808208 [https://perma.cc/LY5L-MP9W].

[12] Dror-Shpoliansky & Shany, *supra* note 6, at 1251.

entirely.[13] For example, Dror-Shpoliasky and Shany offer a replacement paradigm that considers three generations of human rights digitally manifesting in distinct phases to (1) adjust transference, (2) recognize new right, and (3) vest rights in digital personae directly:

> • The first generation involves far-reaching processes of adjustment of offline human rights to the online world.
>
> • The second generation features the emergence of new digital human rights—that is, rights that protect online needs and interests that do not have close parallels in the offline world. Although second-generation rights may be genealogically traced back to existing offline human rights, the new progenies are not fully subsumed in the human rights from which they originate.
>
> • The third generation comprises rights belonging to new online personae—that is, digital or virtual representations of natural persons or legal entities that exist and exercise rights separately from the human beings or legal entities that created them. This third generation of rights is also expected to focus more and more attention on the direct human rights obligations of technology companies exercising de facto governance power over the online user.[14]

While this framework is both interesting and forward-looking, it nevertheless, ignores the main value of the existing paradigm supported by the United Nations and other human rights entities[15]—namely the near universal acceptance of what our human rights actually are. In theory, if not in practice, human rights are *sine qua non* and obtain everywhere humans are.

Building on a 2012 resolution by the U.N. Human Rights Council proclaiming that "that the same rights that people have offline must also be protected online",[16] this article develops an analytic matrix charting the path of each human right into cyberspace as Internet human rights. Structurally,

---

[13] *Id.* at 1256–57.
[14] *Id.* at 1252.
[15] *Id.* at 1251, 1265–66 (discussing concerns over the normative equivalency paradigm embraced by the United Nations and proposing a new framework with new digital rights). We do not take sides in the debate over "normative equivalence" central to Dror-Shlopinasy & Shany's thesis; nor do we question whether "new" digital rights are in order.
[16] Human Rights Council Res. 20/8, U.N. Doc. A/20/8, at 2 (July 5, 2012).

our matrix tracks the migration of articles in the Universal Declaration of Human Rights (UDHR)[17] from the physical world into the digital world.[18] To be sure, mapping the UDHR to cyberspace is a task fraught with interpretive nuance and missed digital rabbit holes. Moreover, this exercise must acknowledge new precursor "digital core rights" that are necessary preconditions to effectuating Internet human rights: connectivity and net neutrality.

Championed by intergovernmental organizations such as the United Nations, Internet Governance Forum (IGF), and the Internet Corporation for Assigned Names and Numbers (ICANN)[19] as well as international financial institutions such as the World Bank,[20] connectivity seeks to ensure access by everyone to the Internet.

As such, "connectivity" functions as a key core right—without which all the other rights cannot fully exist. If one is not connected to the Internet, then free speech, free association, free practice of religion and other "active" rights cannot be effectuated, although more passive rights such as privacy may not require connectivity.[21] Even Mark Zuckerberg has asserted that Internet

---

[17] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948) [hereinafter UDHR].

[18] Similar work has been done tracking the migration the Geneva Convention's laws of war into cyberspace. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., Cambridge Univ. Press 2d ed. 2017).

[19] U.S. DEP'T OF STATE, U.S. INTERAGENCY STEERING GROUP REPORT 3 (2016) (describing the Global Connect Initiative, launched by the U.S. Department of State "based on the notion that all stakeholders, including governments, the private sector, civil society, multilateral development banks, and international organizations, must play their part to expand connectivity"); Ashwin Rangan, *ICANN IMRS Cluster Brings a More Resilient and Stable Internet to Africa*, ICANN Blog, Dec. 6, 2022; Junhua Li, Statement, *Universal, Affordable and Meaningful Connectivity*, Internet Governance Forum (2022), https://www.un.org/en/desa/internet-governance-forum-2022.

[20] U.S. INTERAGENCY STEERING GROUP REPORT, *supra* note 19; *Connecting for Inclusion: Broadband Access for All*, THE WORLD BANK https://www.worldbank.org/en/topic/digitaldevelopment/brief/connecting-for-inclusion-broadband-access-for-all [https://perma.cc/D3SG-7UUS] (last visited Apr. 13, 2023).

[21] *See* Dror-Shpoliansky & Shaby, *supra* note 6, at 1280 (asserting that "connectivity" should be considered a "new" right); THE CHARTER OF HUMAN RIGHTS AND PRINCIPLES FOR THE INTERNET, THE INTERNET RIGHTS & PRINCIPLES DYNAMIC COALITION (Marianne Franklin, Robert Bodle & Dixie Hawtin eds., 4th. ed. 2014) ("Access to and use of the Internet is increasingly indispensable for the full enjoyment of human rights . . . .") https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf.

access is a human right.[22] Public polling data shows that many people agree with him.[23] That said, connectivity itself is not just access to the Internet. Nor is it free. Connectivity implies derivative rights such as electrical power, a telecommunication grid, satellite access, and access to computer hardware and software. Thus, access, connection, and realization of digital human rights go hand in hand.[24]

The second precursor right, net neutrality, *i.e.*, every human enjoys similar digital service with respect to speed and content, is a secondary core right, folded into the digital emergence of human rights such as equality and freedom from discrimination. Once connectivity is achieved, each Internet user should, in principle, have the same digital experience—which requires Internet Service Providers (ISPs) to treat all communications equally.

This principle sits uneasily alongside basic concepts of capitalism that would allow an ISP, as a private corporation, to offer different Internet services and speeds at different price points to different classes of customers based upon the profit that can be achieved at each level. By not allowing ISPs to discriminate in either treatment or price based upon the content, user, application, source/destination address or other basis, state regulators move further toward treating ISP's as public utilities.

The UDHR was the first global articulation defining human rights and is easily the most renowned international human rights instrument. It reflects the drafters' assertion that "human rights are part of people's moral DNA . . . ."[25] Conceptually, this moral basis for modern human rights rooted millennia ago as philosophers struggled to discern natural law. "Natural law thinkers, Cicero among them, viewed the world as webbed together by a single, universal set of moral principles, regardless of how fissioned into different political and cultural units humanity might be."[26] Universality, then, is the bridge marrying our "moral DNA" to what is now becoming our digital DNA.

---

[22] Jessi Hempel, *Zuckerberg to the UN: The Internet Belongs to Everyone*, WIRED (Sept. 28, 2015, 10:39 AM), https://www.wired.com/2015/09/zuckerberg-to-un-internet-belongs-to-everyone/ [https://perma.cc/Y2LU-WRNM].

[23] *Internet Access is 'a Fundamental Right'*, BBC (Mar. 8, 2010, 8:52 AM), http://news.bbc.co.uk/2/hi/technology/8548190.stm [https://perma.cc/XR3U-DH3V].

[24] *See* Nicola Lucchi, *Internet Content Governance and Human Rights*, 16 VAND. J. ENT. & TECH. L. 809, 821 (2014).

[25] JOHANNES MORSINK, ARTICLE BY ARTICLE: THE UNIVERSAL DECLARATION OF HUMAN RIGHTS FOR A NEW GENERATION 1 (2022).

[26] CRAIG FORCESE, DESTROYING THE CAROLINE: THE FRONTIER RAID THAT RESHAPED THE RIGHT TO WAR (2018) at 131 (*citing* STEPHEN NEFF, WAR AND THE LAW OF NATIONS: A GENERAL HISTORY (2005) at 10, 32.).

Those centuries-old, morally-based, natural law roots took full flower through the international community's adoption of the UDHR. As such, we use it here as a proof-of-concept for our digital human rights mapping project.

We are cognizant, of course, that other instruments, such as the International Covenant on Civil and Political Rights (ICCPR)[27] and International Covenant on Economic, Social and Cultural Rights (ICESCR)[28] also reflect the rights contained in the UDHR, carry those rights into legal force with the exception of Article 17 (property),[29] and could and should also be similarly analyzed;[30] however, we believe it important to first establish a sound methodological framework before applying it to other instruments.

It must also be noted that in this article we do not analyze in-depth the substance of each right in depth [31] but rather attempt to show how such rights as generally understood would "map" to the Internet. Also, while certain rights (such as Article 12 on privacy and Article 19 on freedom of expression) might more easily be "transposed" from their analogue origins to applicability in the Internet context (and while some of these have also been the subject of specific examination by Special Rapporteurs)[32], we have resisted the temptation to organize these rights according to how directly or indirectly they might be mapped to the Internet context.

In the months and years ahead, especially as virtual reality (VR), augmented reality (AR) and gaming gain traction through the "metaverse," it is easy to predict that case law and regulation will address issues that arise in those contexts; what is more difficult to predict is how those rights which are perhaps not directly applicable today might be viewed legally in the future. Additionally, as discussed below, some rights might be in conflict with one another when applied to cyberspace, and while we note these instances, we do not attempt to resolve them here.

---

[27] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.
[28] International Covenant on Economic, Social and Cultural Rights, Dec. 16, 1966, 993 U.N.T.S. 3.
[29] MORESINK, *supra* note 25, at 16.
[30] *See* Pedro Pizano, *The Human Rights That Dictators Love*, FOREIGN POLICY (Feb. 26, 2014, 3:45 PM), https://foreignpolicy.com/2014/02/26/the-human-rights-that-dictators-love/ [https://perma.cc/9XPK-CDTW] (explaining how states allocated certain rights contained within the non-binding UDHR into the binding ICCPR and ICESCR).
[31] Other scholars have done so. *See generally* THE UNIVERSAL DECLARATION OF HUMAN RIGHTS (William A. Schabas ed., 2013); Steven L.B. Jensen, THE MAKING OF INTERNATIONAL HUMAN RIGHTS (2016).
[32] *See* Appendix for a non-exhaustive list of Reports from Special Rapporteurs attempting to tackle this issue.

Finally, as is demonstrated by the discussion below, especially around remedies and the "right to be forgotten,"[33] this article identifies for further study the growing "multi-stakeholderisation" of the enforcement of human rights online.[34] In other words, the assignment of certain regulatory and enforcement responsibilities to non-state actors such as multinational tech corporations which occupy or control discreet portions of cyberspace to the effective exclusion of others.

The Matrix of Internet Human Rights

Our matrix tracks migration of each human right defined in the UDHR, as refined by the United Nations' Office of the High Commissioner for Human Rights,[35] from the kinetic into the digital world. Some rights, such as freedom of expression, privacy, and equality, have progressed much farther than others. Equally apparent, some rights are more digitally "transferrable" than others. As we scan the international and domestic regulatory environments, the matrix reflects positive significant manifestation, codification, regulation, or enforcement. Unfilled spaces in the matrix reflect either insignificant realization, no movement, or negative regulation—i.e. prohibition or significant restriction.

Articles 12 and 13 demonstrate this approach. Article 12's right to privacy— articulated, implemented, and enforced by the European Union as the "right to be forgotten"—ticks all four cells of the matrix, accompanied by descriptive terms. Article 13's freedom of movement in cyberspace enjoys little positive manifestation because international law and most western societies presume it; thus, no cells are ticked. However, as any visitor to the

---

[33] *See* discussion of UDHR art. 12 *infra* p. 9; Kelly & Satola, *supra* note 7, at 1 (discussing European authorities' assignment of oversight responsibilities to Google).

[34] One example of an effort to bring together multiple stakeholders to advance digital human rights is the Human Rights and International Law Working Group (HRILWG) of the Government Advisory Committee (GAC) of ICANN. ICANN is a California not-for-profit corporation, and the HRILWG is charged to, inter alia, "…encourage and facilitate multi-stakeholder support and cooperation in advancing human rights related policies, recommendations, and advice…" *GAC Working Group on Human Rights and International Law (HRILWG)*, ICANN, https://gac.icann.org/working-group/gac-working-group-on-human-rights-and-international-law-hrilwg [https://perma.cc/GT3N-2XPP] (last visited Mar. 30, 2023).

[35] *30 Articles on the 30 Articles of the Universal Declaration of Human Rights*, OFF. OF THE HIGH COMM'R FOR HUM. RTS., (Nov. 14, 2018), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23871&LangID=E [https://perma.cc/V6MC-266G].

United Kingdom knows, one must "mind the gap." Such lack of significant positive regulation leaves room for negative regulation. In the case of Article 13, certain states have significantly limited freedom of movement in cyberspace across websites. Although not appearing on the matrix, these negative regulatory trends are discussed in the commentaries that follow.

The scope of our analysis is necessarily broad and evolving. Many areas and themes are untested in terms of case law or regulation. So, while the authors provide a framework, this mapping project is necessarily a snapshot in time. Examples will continue to arise, such as Elon Musk's recent purchase of Twitter, bringing a significant online free speech platform under the sway of a single personality given the nature of its private incorporation.[36] In that sense, this work should not be seen as exhaustive, but rather a working hypothesis for an analytical approach.

[36] *See generally* Kate Conger, *How Twitter Will Change as a Private Company*, N.Y. TIMES (Oct. 28, 2022), https://www.nytimes.com/2022/10/28/technology/twitter-changes.html [https://perma.cc/28DK-S3JF].

UDHR Article	Digital Manifestation	Codification	Regulation	Enforcement
1. Freedom and Equality	✓ As Connectivity ✓ As Net Neutrality	In Progress…	In Progress…	
2. Freedom from Discrimination	✓ Re: Cyber-bullying	✓ Re: Cyber-bullying	In Progress…	
3. Right to Life, Liberty, Security	✓ Re: Online Identity	✓ Re: Identity Theft	In Progress…	✓ Per States
4. Freedom from Slavery	✓ Re: Human Trafficking	✓ Criminalization	✓ Via Prosecution	✓ Per States
5. Freedom from Torture	✓ Re: Cyber-bullying as psychological torture	✓ Criminalization re: targeted children	✓ Via Prosecution	✓ Per State Law Enforcement
6. Recognition Before the Law	✓ As Digital Persona		✓ Via Tech Corp.'s	✓ Per Terms of Service
7. Right to Equality Before the Law	✓ As Connectivity by avoiding shutdowns			✓ Per Alternate Tech platforms
8. Right to Remedy	✓ For enforceable Internet H.R.'s			✓ Re: each enforceable Internet H.R.
9. Freedom from Arbitrary Detention	✓ Re: Prisoner Internet access rights			✓ Per State incarceration rules
10. Right to a Fair Trial	✓ As Defendant rights in cyber-crime cases	✓ As Defendant's civil rights	✓ Via State Courts	✓ Via State Courts
11. Presumption of Innocence				
12. Right to Privacy	✓ As RTBF	✓ As EU Regulation	✓ Via EU states	✓ Via ECJ
13. Freedom of Movement				
14. Right to Asylum	✓ As VPN Access			
15. Right to Nationality	✓ As Benefits access			
16. Right to Marry and Found a Family	✓ As Online dating, weddings, family life		✓ Via Tech Corp.'s	✓ Per Terms of Service
17. Right to Property	✓ As Digital Property	✓ Per TRIPS for IP	✓ Via States	✓ Via States
18. Freedom of Religion	✓ As Religious Surfing			
19. Freedom of Opinion/Expression	✓ Access to Social Media Platforms		✓ Via Tech Corp.'s	✓ Per Terms of Service
20. Freedom of Assembly	✓ Access to Groups		✓ Via Tech Corp.'s	✓ Per Terms of Service
21. Democratic Participation	✓ As Electronic voting	✓ Per State laws	✓ Via States	✓ Via States
22. Right to Social Security	✓ As Self-realization			
23. Right to Work	✓ Re: Teleworking	✓ In progress…		
24. Right to Rest/Leisure				
25. Right to Adequate Standard of Living	✓ Re: Reproductive healthcare			
26. Right to Education	✓ Re: Remote learning	✓ Compulsory education laws	✓ Via Education authorities	✓ Via States
27. Right to Cultural, Art, Sci.	✓ As Remote access			✓ Per Museum policy
28. Right Social Order	✓ In progress… via states or tech corp.'s			
29. Duty to Community				
30. Rights are Inalienable				

Figure 2 Matrix for Digital Manifestation of Human Rights

UDHR Preamble

Establishing that human rights are universal, vested in people, and to be observed, the UDHR's Preamble states:

> [T]he General Assembly proclaims this universal declaration of human rights as a common standard of achievement for all peoples and all nations, to the end that every individual and every organ of society, keeping this Declaration constantly in mind, shall strive by teaching and education to promote respect for these rights and freedoms and by progressive measures, national and international, to secure their universal and effective recognition and observance, both among the peoples of Member States themselves and among the peoples of territories under their jurisdiction."[37]

Applied to the Internet, the language requiring "every organ of society" take progressive measures and secure these rights would appear to call upon not only governments, but Internet service providers and other organizations in the tech sector to do their part. This interpretation clearly fits with the mandate placed on Google by the ECJ to effectuate the right to privacy in cyberspace as the right to be forgotten.[38]

With respect to the question of *where* the Internet actually is, cyberspace is a conundrum. It could analogously be a "territory" under the jurisdiction of Member States.[39] As such, there is at once a physical and digital component and a technical limit to what State X may be able to do in securing and enforcing the human rights listed.[40] Due to the Internet's structure, routing and re-routing based on systems with built-in layers of redundancy, the Internet itself may in fact limit the leeway State X has in controlling the cyberspace being used by its people. That said, cyberspace is not fully a global commons either. Unlike the high seas or outer space, parts of it are regulated directly by state actors and international organizations such as

---

[37] UDHR, *supra* note 17, pmbl.
[38] Kelly & Satola, *supra* note 7, at 6.
[39] *But see* David R. Johnson & David G. Post, *Law and Borders—The Rise of Law in Cyberspace*, 45 STAN. L. REV. 1367, 1369 (1996) (arguing the futility of efforts to govern the flow of cyberspace across territorial bounds).
[40] Eric T. Jensen, *Cyber Sovereignty: The Way Ahead*, 50 TEX. INT'L L.J. 275, 277–78 (2015).

ICANN. Moreover, some states are attempting to segment and control portions of it to erect parallel Internets more fully under their control.[41]

Article 1: Freedom and Equality

Equality on the Internet, or "cyber-equality," can be achieved through Article 1, which 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.[42]

If net neutrality is a core right that is a precursor to the digital existence of other human rights, then its home is in Article 1 of the UDHR. Freedom and equality are both implicated if connectivity, restricted access once online, speed, and bandwidth are determined by political, financial, geographic, categorical, or other means. In many ways, the equality of access issue mirrors equality issues in the physical world related to discrimination. For example, in the United States, where a digital divide regarding Internet access exists between minority and non-minority populations creates a type of "cyber segregation," it has been argued that the 14th Amendment should obligate equal access to technology.[43]

---

[41] Madhumita Murgia & Anna Gross, *Inside China's Controversial Mission to Reinvent the Internet*, FIN. TIMES (Mar. 27, 2020), https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f [https://perma.cc/DWT7-584G]. For a fuller discussion, see generally ROGIER CREEMERS, *China's Conception of Cyber Sovereignty: Rhetoric and Realization*, *in* GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY 107–31 (Dennis Broeders & Bibi van den Berg eds., 2020).

[42] UDHR, *supra* note 17, at art. 1.

[43] Kenneth Sharperson, *The Digital Divide: Modern Day Jim Crow?*, 205 N.J. LAW. 50, 50 (Oct. 2000). *See also*, U.S. CENSUS BUREAU, *The Digital Divide: Percentage of Households by Broadband Internet Subscription, Computer Type, Race and Hispanic Origin*, CENSUS GOV (Sept. 11, 2017), https://www.census.gov/library/visualizations/2017/comm/internet.html [https://perma.cc/RWH8-FRUX]. For discussion of the digital divide internationally, see Mukhisa Kituyi, *The Digital Divide Is Impeding Development*, UNITED NATIONS CONF. ON TRADE & DEV. (Oct. 24, 2018), https://unctad.org/news/digital-divide-impeding-development [https://perma.cc/6RK5-JUMR]; (Oct. 24, 2018); Tom Curran, *The Digital Divide in Developing Nations: Policy Impact on the Internet in Sub-Saharan Africa*, CHI. POL'Y REV. (Apr. 12, 2017), https://chicagopolicyreview.org/2017/04/12/the-digital-divide-

Rural and low-income communities also fall on the wrong side of this divide.[44] According to the U.S. Census Bureau, COVID-19 further exasperated these problems due to many schools moving to an online only format. During this time, lower income families and minority, non-white households were much less likely to report computer and internet availability than high income white households.[45]

Notwithstanding inequality within countries such as the United States, adoption and enforcement of net neutrality policies vary widely across countries. For example, the European Union has moved determinedly in the direction of net neutrality. By 2016, the European Union had reissued continent-wide telecoms rules that established a framework through Member State cooperation, ensuring net neutrality throughout the European Union.[46] While some argued that loopholes built into the regulation allowed ISP's to defeat net neutrality,[47] the baseline provisions allowed Member States to enact even stronger net neutrality provisions. The Netherlands and Slovenia, for example, have taken advantage of that provision[48].

Conversely, in the United States the debate is unsettled.[49] The United States made strides in this direction when the FCC under President Obama adopted the Open Internet Order in 2015[50] setting "federal regulations to

---

in-developing-nations-policy-impact-on-the-internet-in-sub-saharan-africa/ [https://perma.cc/7GCN-QM6B].

[44] Emmanuel Martinez, *How Many Americans Lack High-Speed Internet?*, THE MARKUP (Mar. 26, 2020, 10:05 AM), https://themarkup.org/the-breakdown/2020/03/26/how-many-americans-lack-high-speed-internet [https://perma.cc/JR6T-T5MC].

[45] U. S. CENSUS BUREAU, *Week 5 Household Pulse Survey: May 28 - June 2, Education Table 2: COVID-19 Pandemic Impact on How Children Received Education, by Select Characteristics*, CENSUS GOV (June 10, 2020), https://www.census.gov/data/tables/2020/demo/hhp/hhp5.html [https://perma.cc/C7DW-8EYT]..

[46] 2015 O.J. (L 310/8) 3.

[47] Alex Hern, *EU Net Neutrality Laws Fatally Undermined by Loopholes, Critics Say*, THE GUARDIAN (Oct. 27, 2015) https://www.theguardian.com/technology/2015/oct/27/eu-net-neutrality-laws-fatally-undermined-by-loopholes-critics-say [https://perma.cc/5V79-Y27Y].

[48] Ot van Daalen, *Translation of Key Dutch Internet Freedom Provisions*, BITS OF FREEDOM (June, 27, 2011), https://www.bitsoffreedom.nl/2011/06/27/translations-of-key-dutch-internet-freedom-provisions/ [https://perma.cc/J3TH-BWSV; EDRi, *Slovenia has a New Net Neutrality Law*, EDRI (Jan. 30, 2013), https://edri.org/our-work/edrigramnumber11-2slovenia-net-neutrality/ [https://perma.cc/USC6-K68B].

[49] Chris Linebaugh, *Net Neutrality Law: An Overview*, CONG. RESEARCH SERVICE REP. (Oct. 18, 2022).

[50] Protecting and Promoting the Open Internet, 80 Fed. Reg. 19,737 (proposed April 13, 2015).

prohibit Internet service providers from blocking, throttling, or unfairly prioritizing Internet traffic."[51] However, this regulatory effort was undone under President Trump when the FCC later adopted the Restoring Internet Freedom Order in 2018.[52] The legal difference concerned classifying ISP's under Title II of the 1934 Communications Act as amended in 1996[53] as "telecommunications services" and therefore more tightly controlled, or classifying them under Title I as "information services" and therefore less tightly controlled.[54] The Biden administration is moving to return to the Obama era regulatory approach.[55]

Although net neutrality has been backed by the United Nations at the international level,[56] adoption and enforcement remain at the national level,[57] creating unevenness which jeopardizes implementation of this right—especially where weaker rules are in effect over a territory through which significant traffic is routed. For example, while Chile and Brazil have strong net neutrality provisions within their own borders, because approximately 90% of Latin America's Internet traffic routes through Florida, as a practical matter, the United States' weakened net neutrality FCC rules under the Trump administration could have rendered those national policies in Chile and Brazil essentially meaningless.[58]

Beyond addressing the unevenness problem, another reason to internationalize net neutrality standards is to bring uniformity to the exceptions. Thus, while Qatar, India, and Turkey have been identified by the

---

[51] Caitlin Chin, *In the Net Neutrality Debate, What Might Follow Mozilla v. FCC?*, BROOKINGS: TECHTANK, (Oct. 7, 2019), https://www.brookings.edu/blog/techtank/2019/10/07/in-the-net-neutrality-debate-what-might-follow-mozilla-v-fcc/ [https://perma.cc/QBA4-Z6ET].

[52] Restoring Internet Freedom Order, 83 Fed. Reg. 7852 (proposed Feb. 22, 2018).

[53] Communications Act of 1934, 47 U.S.C. § 151 (1996).

[54] Chin, *supra* note 51. For an in-depth discussion of the implications between these two classifications for ISP's, see Mozilla v. FCC, 940 F.3d. 1 (D.C. Cir. 2019)

[55] Lauren Feiner, *Net Neutrality is Poised for a Comeback as Biden Tries to Get Last FCC Commissioner Confirmed*, CNBC: TECH (Dec. 21, 2021), https://www.cnbc.com/2021/12/21/net-neutrality-to-return-as-senate-weighs-confirming-gigi-sohn-for-fcc.html [https://perma.cc/P59U-JKX6].

[56] Human Rights Council Res. 32/13, U.N. Doc. (A/HRC/RES/32/13) (July 18, 2016).

[57] *OECD Communications Outlook 2013*, Table 2.9, 2013, https://www.oecd.org/sti/broadband/2-9.pdf.

[58] Nancy Scola, *How U.S. Net Neutrality Could Be an International Human Rights Fight*, WASH. POST (Dec. 10, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/10/how-net-neutrality-could-be-a-human-rights-issue/ [https://perma.cc/J22U-M8D2].

U.N. Human Rights Council as infringing on Internet access under pretext,[59] France, the United Kingdom, and other Western states have used intellectual property protection (specifically the so-called "three-strikes" standard) for restricting Internet access against those caught violating copyright protections – either for limited periods of indefinitely.[60]

In France, HADOPI, a new governmental agency was created, to enforce the three-strike rule. For the first offense, HADOPI sends a warning via email, notifying the offender of the alleged violation, where to find clarifying information, and the penalty for further offenses. After the second offense, a warning via email is coupled with a certified letter (receipt acknowledged) with the same information as above. Once a third offense detected, HADOPI may commence a procedure against the offender which could end in a fine or suspension of access to the Internet.[61]

Thus, although state policies are trending in the right direction, for Article 1's promise of equality to manifest digitally, more states must move forward with net neutrality and connectivity commitments to complement the international policies of institutions such as the World Bank, IMF, and U.N. agencies. Evenness in application should undergird this manifestation, which could perhaps be better achieved through agreed minimum standards such as those which form a foundational basis in areas such as trade, labor, banking, air traffic, and weights and measures.

Article 2: Freedom from Discrimination

Freedom from discrimination dovetails with freedom and equality, secured through net neutrality. Article 2 states:

> Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social

---

[59] Jillian York, *UN Human Rights Council Resolution on Internet and Human Rights a Step in the Right Direction*, ELEC. FRONTIER FOUND. (July 26, 2012), https://www.eff.org/deeplinks/2012/07/un-human-rights-council-resolution-internet-and-human-rights-step-right-direction [https://perma.cc/2XKX-F5PC].

[60] David W. Quist, *Three Strikes and You're Out: A Survey of Foreign Approaches to Preventing Copyright Infringement on the Internet*, 66 BUSINESS LAWYER 261, 261 (Nov. 2010); Primavera De Filippi & Daniele Bourcier, *'Three-Strikes' Response to Copyright Infringement: The Case of Hadopi*, *in* THE TURN TO INFRASTRUCTURE IN INTERNET GOVERNANCE (Francesca Musiani et al. eds., 2016), Available at SSRN: https://ssrn.com/abstract=2728653 [https://perma.cc/8X4W-HV48].

[61] Filippi & Bourcier, supra note 60, at 126–127 134–135.

> origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.[62]

Adapted to the Internet, this right overlaps with cyber-bullying and net neutrality—bullying on the basis of race, gender, or other protected classification, or discrepancy in access to the Internet on similar bases. It also implicates online sexual harassment,[63] depending upon whether discrimination/harassment laws have been updated in the face of technological advancements such as the Internet – which is not always the case.[64] The key to successful enforcement of the digital version of this prohibition on discrimination will lie in the answer to the question of whether individuals are only protected from such forms of discrimination by their governments or are they also protected from similar conduct by private actors such as corporations and other individuals.

Australia's Racial Discrimination Act of 1975[65] makes racial hatred unlawful. However, it is "not possible" to apply this act against ISPs or individuals located in other countries.[66] In *Jones v. Toben*, the Federal Court of Australia found this legislation to be capable of combating online race hate material when (1) an author of online material can be identified and (2) the online material is hosted by an Australian ISP. In the case, the Adelaide Institute had published material on its website which constituted "malicious anti-Jewish propaganda." The website, maintained by Dr. Toben, denied the existence of the Holocaust and blamed Jews for the crimes of Stalin. Toben was an Australian citizen posting to a site hosted by an Australian ISP. The court ordered Toben to remove the offending material.[67]

---

[62] UDHR, *supra* note 17, at art. 2.
[63] Mary Anne Franks, *Sexual Harassment 2.0*, 71 MD. L. REV. 655, 678 (2012).
[64] Marlisse Sweeney, *What the Law Can (and Can't) Do About Online Harassment*, THE ATLANTIC: TECH (Nov. 12, 2014), https://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638/ [https://perma.cc/4R43-2KAG].
[65] *Racial Discrimination Act 1975* (Cth) pt IIA (Austl.).
[66] *Cyber-racism Symposium Report*, AUSTL. HUM. RTS. COMM'N (2002), https://humanrights.gov.au/our-work/cyber-racism-symposium-report#2a [https://perma.cc/B9N8-QJGT].
[67] *See generally Jones v Toben* (2002) FCR 1150 (Austl.).

Interestingly, Dr. Toben had been previously detained, prosecuted, and imprisoned in Germany during December 2000 for publishing the same material on the Adelaide Institute website. Toben was arrested while visiting Germany for a conference and the German court did not find his Australian citizenship or the fact that the website server was located in Australia to be a valid defense.

There are at least three reasons cyberspace itself exacerbates the impact of bullying or harassment: Anonymity, amplification, and permanence.

- **Anonymity**—anonymous attacks are possible online, making remedies or legal action difficult.
- **Amplification**—harassers can find victims quickly and to connect with others who will join in harassment.
- **Permanence**—some online attacks are difficult to erase (e.g. doxing or sharing a victim's personal information, like home address and telephone numbers).[68]

With respect to anonymity, legal action in court can produce results that can lead to addressing the problem. In the case of *Cohen v. Google,*[69] Vogue magazine cover model Liskula Cohen successfully sued Google in New York state court, forcing the company to reveal the identity of an anonymous blogger who was posting hateful and harassing speech directed at her. The material was not only damaging to her emotionally, it also impacted her ability to find work.[70] Once Google reluctantly revealed the identity of the blogger, Cohen's legal team was able to begin the process of building a defamation suit.[71]

According to a 2017 study by the Pew Research Center, four in ten Americans reported having personally experienced online harassment. Nearly one in five Americans reported being subject to severe online harassment including sexual harassment or stalking. PEW's survey demonstrated that cyber harassment typically targets a personal or physical characteristic, like race or ethnicity and gender. It also showed that Americans were divided on the issue of whether protecting free speech or

---

[68] Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 COLUM. J. GENDER & L. 224, 255-56 (2011).
[69] Cohen v. Google, 887 N.Y.S.2d 424, 425–26 (2009).
[70] *Id.* at 426.
[71] Rich McHugh & Noel Hartman, *Model Liskula Cohen Wins Court Battle with Google to Learn Blogger's Identity*, ABC (Aug. 18, 2009, 9:37 PM), https://abcnews.go.com/GMA/story?id=8359356 [https://perma.cc/BBJ7-CEAL].

preventing severe online harassment is more important. 45% of Americans said it is "more important to let people speak their minds freely online" while 53% agreed that it is more important for people to "feel welcome and safe online."[72]

Of particular concern is the vulnerability of youth, who are more frequently victims of discrimination on social media sites like Facebook, Twitter, or YouTube.[73] Within this group, minority youth are more at risk not only because of their minority status, but also because of the amount of time they spend online: "95 percent of youth have access to the [I]nternet . . . and . . . adolescents of color spend 4½ more hours per day on average than their white counterparts using various forms of media, including mobile devices. . . ."[74] Moreover, the numbers are on an upward trend. [75]

With respect to racism, it may be that the Internet itself has become essential for racism to thrive and spread because: (1) racist groups have no access to traditional civilian mass media, and the Internet provides them with a platform, (2) they are often internationally organized and the Internet connects people easily from across the world, (3) Internet technology is easy and available at low costs, and (4) repression of racist Internet activity is not efficient, thereby discouraging governments from seeking enforcement against it. [76] Some have even argued that it is beyond the capacity of the nation-state as a political unit to control the Internet by means of unilateral state regulation.[77]

The Council of Europe has addressed this at the international level with adoption of the Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems in 2006. The Protocol is enforced by signatory states, which agree to criminalize within their jurisdictions

---

[72] Maeve Duggan, *Online Harassment 2017*, PEW RESEARCH CENTER (July 11, 2017), https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/ [https://perma.cc/AEA5-XS2R].

[73] Brendesha M. Tynes, *Online Racial Discrimination: A Growing Problem for Adolescents*, AM. PSYCH. ASS'N SCIENCE BRIEF (Dec. 2015), https://www.apa.org/science/about/psa/2015/12/online-racial-discrimination [https://perma.cc/MN9M-HPGX].

[74] *Id.*

[75] *Id.*

[76] Henrik W.K. Kaspersen, *Cyber Racism and the Council of Europe's Reply*, AUSTRALIAN HUM. RTS. COMM'N, https://humanrights.gov.au/our-work/cyber-racism-and-council-europes-reply#f1 [https://perma.cc/XR6P-CN49] (last visited Apr. 11, 2023).

[77] YAMAN AKDENIZ, RACISM ON THE INTERNET 72 (2009).

dissemination of racist and xenophobic threats, insults, propaganda and other materials via computer systems. It is noteworthy that certain articles in the Protocol are targeted at particularly virulent and prevalent online manifestations of discrimination. For example, Article 5 specifically addresses hate crimes and Article 6 protects against Holocaust denial and the denial of other genocides recognized by international tribunals.[78]

Language in the Protocol's preamble "[s]tressing the need to secure a full and effective implementation of all human rights without any discrimination or distinction, as enshrined in European and other international instruments"[79] implicitly recognizes that this particular international agreement transports the human right of freedom from discrimination from the physical into the digital realm. Currently 34 States have ratified the Protocol or acceded to it, and an additional 11 have signed but not yet ratified.[80]

Yet states are still acting at the state level, despite the expanding international dynamics of this problem. Other rationales for states to restrict xenophobic and racist online discourse may include preservation of public order and protection of the rights of others. Thus, states may restrict discriminatory content by regulating the platform rather than the content itself. In Tanzania, the Cybercrimes Act of 2015 prohibits the production and distribution of racist and xenophobic material[81]

Consequently, although there is regulatory activity in progress surrounding the definition and prohibition of online discrimination, the effective enforcement of this Internet human right will require constant and creative vigilance, special consideration for protecting women and youth minorities, and pressure for technological innovation by social media providers to monitor and regulate their content.

Article 3: Right to Life, Liberty, Security

[78] Additional Protocol to the Convention on Cybercrime art. 5, Jan. 28, 2003, E.T.S. No. 189; *Id.* at art. 6.
[79] *Id.* at pmbl.
[80] *Id., and see* Chart of signatures and ratifications of Treaty 189; Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of racist and xenophobic nature committed through computer systems (ETS o. 189); Status as of 30/04/2023; available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=189 . .
[81] Hanibal Goitom, *Tanzania: Cybercrimes Bill Enacted*, LIB. OF CONG. (June 15, 2015), https://www.loc.gov/item/global-legal-monitor/2015-06-15/tanzania-cybercrimes-bill-enacted/ [https://perma.cc/XH5X-2QBK].

The phraseology of Article 3 includes both a literal and virtual meaning as it exists on the Internet:

> Everyone has the right to life, liberty and security of person.[82]

Unfortunately, the literal version can and has led to mass death in the physical world. This version manifests when a group takes control of key aspects of the Internet to direct conduct in the physical world leading to mass human suffering, not unlike use of the radio in Rwanda in connection with the 1994 genocide.[83]

If Article 3's right to life means anything, it should at least mean the right to continue actually living. Targeted propaganda spread via the Internet to undermine the right to life, leading to mass death in the physical world, is not only a violation of this human right in the civil law context, but also a crime against humanity in the criminal law context. As previously discussed in the case of Article 2's protection against discrimination, racial denigration via the Internet can have real-world consequences. This simultaneously underscores the increasingly inseverable connection between these two worlds, and the need for effective protections in both.

Aside from the physical version of life, the virtual version of life protected by Article 3 exists in the form of one's online identity—an avatar in VR, AR or a computer game, an online personality on a blog, an entertainer or comedian with an alternative personality, etcetera. This is an area where case law will undoubtedly evolve in the near future. Are these digital forms of oneself imbued with similar protections of life, liberty, and security? Many argue yes, and some states have moved to regulate conduct compromising them. Violations of this right commonly take the form of hacking/identity theft, harassment of the virtual being, and deep fakes. While freedom from harassment has been acknowledged as both a problem to be addressed and a right to be protected, it has not been fully transferred and protected in cyberspace as has the protection of one's identity—the violation of which can trigger criminal sanctions if issues surrounding attribution can be overcome.

The segment of the Internet populated by video game usage and interaction presents unique opportunities, depending upon the parameters of the game, for sexual harassment—multi-player VR, environments especially

---

[82] UDHR, *supra* note 17, at art. 3.

[83] *Rwanda Radio Transcripts*, Montreal Inst. for Genocide & Hum. Rts. Stud., https://www.concordia.ca/research/migs/resources/rwanda-radio-transcripts.html [https://perma.cc/PGB7-QBDH].

so.[84] Instances of female avatars, played by women, being sexually assaulted by male avatars, can, because of the more immersive virtual technology, produce heightened abuse trauma as in the victims as "the line between our real bodies and our digital bodies begin to blur."[85]

Game developers have been known to step in to regulate this conduct when they learn of it. For example, when a female gamer complained online of the trauma she experienced after her avatar was repeatedly groped and harassed by another player's avatar while playing the virtual reality game QuiVR, the game developers "updated the game's code to include an expanded 'personal bubble'" that can be activated by the player's avatar with a "power gesture" to protect them from such harassment.[86]

This protection is an example of a private sector actor self-regulating a digital platform to effectuate the security aspect of Article 3's right to life, liberty, and security—even absent a government mandate to do so. In fact, since corporations own the environments within which such conduct might occur, this will likely be the more common mode of enforcement. Companies such as Microsoft have published "community standards" for gamers on Xbox that prohibits such conduct.[87]

A 2019 study by the Anti-Defamation League found that 53% of people who reported experiencing harassment were targeted for their "race, religion, ability, gender, gender identity, sexual orientation, or ethnicity."[88] However, researchers argue that women are especially targeted and when gender-based sexual harassment is downplayed by advising people to simply get off-line from the offending conduct, reporting can be hampered.[89] Unfortunately,

---

[84] Julia Carrie Wong, *Sexual Harassment in Virtual Reality Feels All Too Real – 'It's Creepy Beyond Creepy'*, THE GUARDIAN (Oct. 26, 2016, 3:25 PM), https://www.theguardian.com/technology/2016/oct/26/virtual-reality-sexual-harassment-online-groping-quivr [https://perma.cc/F8B5-HTXE].

[85] *Id.*

[86] *Id.*

[87] Dave Smith, *Most People Who Play Video Games Online Experience 'Severe' Harassment, New Study Finds*, BUS. INSIDER (July 25, 2019, 11:08 AM), https://www.businessinsider.com/online-harassment-in-video-games-statistics-adl-study-2019-7 [https://perma.cc/2W2P-3QAQ].

[88] *Id.*

[89] *See* Danielle K. Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 375–76 (2009); *see also Virtual Rape is Traumatic, but Is It a Crime?*, WIRED, (May 4, 2007, 12:00 PM), https://www.wired.com/2007/05/sexdrive-0504/ [https://perma.cc/9J5G-UGPS].

such remedies depend upon attribution of the conduct, and many perpetrators are anonymous.[90]

Online identity theft can be seen as an assault upon the life and security components of Article 3 and occurs into two forms: identity theft for criminal commercial purposes and identity theft via deep fakes to ruin one's reputation or publicly promote another's agenda. While criminalization and enforcement has begun at both the international and domestic levels for the first type, similar regulation has been lagging for the second type, leaving victims with the option of pursuing private causes of action as a legal recourse.

Hacking and identity theft are the most powerful tools via the Internet for taking over another person's life in violation of Article 3. A 2019 study by the online security firm Symantec found that one in ten people are victims of identity theft annually and 21% of them are victimized repeatedly.[91] Recently, hacking has been prevalent in both individual and corporate capacities. On May 7, 2021, Colonial Pipeline, a major pipeline delivering gas, diesel, and jet fuel across the East and Southeast United States, was hacked by a Russian organization called DarkSide.[92] DarkSide had issued a ransom note to Colonial Pipeline, causing the pipeline to shut down for the first time in its 57-year history.[93] The ransom note, demanding around $4.4 million to be paid in crypto currency, was later partially recovered by the Department of Justice's digital extortion task force.[94]

From a regulatory standpoint, many states must approach this issue by adapting the data security laws they already have in place, although that still might not adequately solve the problem. All fifty states in theU.S.have some

---

[90] Tali Arbel, *How to Stop Harassment in Video Games*, SEATTLE TIMES (Mar. 12, 2016, 5:08 AM), https://www.seattletimes.com/business/how-to-stop-harassment-in-video-games/ [https://perma.cc/KN8G-UXM4].

[91] Scott Steinberg, *The Latest Ways Identity Thieves Are Targeting You—And What to Do If You Are a Victim*, CNBC (Feb. 27, 2020, 10:18 AM), https://www.cnbc.com/2020/02/27/these-are-the-latest-ways-identity-thieves-are-targeting-you.html [https://perma.cc/BJD9-CBV7].

[92] William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021, 3:58 PM), https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password#xj4y7vzkg, [https://perma.cc/7NWH-ZWF3].

[93] *Id*.

[94] Evan Perez, Zachary Cohen, & Alex Marquardt, *First on CNN: US Recovers Millions in Cryptocurrency Paid to Colonial Pipeline Ransomware Hackers*, CNN (June 8, 2021, 4:46 AM), https://www.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html [https://perma.cc/CPR2-Y64U].

form of data-breach notification law, which requires that in the event of a data breach that would potentially affect the state's residents, that the holder of such information contact the Attorney General of that state to give notice of the data breach.[95]

Also from a security standpoint, as "Internet of Things" becomes more prevalent, concerns have emerged about inherent security flaws and current data security laws which do not apply.[96] Connecting one's devices to one's smartphone means that often a hacker only has to successfully penetrate the phone to then have access to all other equipment and devices that the phone communicates with regularly. "Cybersecurity experts said it's not that difficult for hackers to gain access to 'internet of things' devices, which include Ring security cameras and voice assistants, such as Alexa and Google Home."[97] Attribution of such crimes to those doing the hacking require an investment of resources that law enforcement may not be willing to commit if the crime occurs on an individual level as opposed to the hack and identity theft of millions of victims when a bank or large retailer like Target are involved.[98]

Consequently, Article 3 human rights are beginning to gain traction with respect to not only protections against identity theft and hacking in addition to increased data protection efforts, but also in the area of online gaming, where virtual aspects of individuals should enjoy freedom of life liberty and security. While the former are government-driven efforts, the latter is ultimately controlled by gaming companies and is enforceable only in accordance with their terms of service. Absent increased state regulation in the gaming space, ensuring Article 3 rights for avatars and other virtual creations by humans will be left up to those companies.

Article 4: Freedom from Slavery

---

[95] *See, e.g.*, NEB. REV. STAT. § 87-803 (2021); ALA. CODE § 8-38-1 et. seq; N.Y. GEN. BUS. LAW § 899-AA.

[96] *See generally* Scott R. Peppet, *Regulation the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85 (2015) (discussing concerns with the growing "Internet of Things" and proposing a regulatory approach to address these concerns).

[97] Neil Vigdor, *Somebody's Watching: Hackers Breach Ring Home Security Cameras*, N.Y. TIMES (Nov. 11, 2020), https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html [https://perma.cc/2SJZ-4A2U].

[98] *See, e.g.*, Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ [https://perma.cc/ST8H-5Q6B] (explaining the 2013 Target data breach, which impacted millions of shoppers).

The UDHR's Article 4 disallows holding people in slavery or servitude and prohibits the slave trade, stating specifically:

> No one shall be held in slavery or servitude; slavery and the slave trade shall be prohibited in all their forms.[99]

While modern manifestations of slavery and servitude include forced labor in multiple situations such as agriculture, domestic service, and mining, the face of both slavery and the slave trade today is Internet-driven human trafficking for the sex trade.[100] Although the Internet was never intended for such use, it has greatly accelerated the growth in sex trafficking of minors.

> In the United States, 2 out of every 3 children sold for sex are trafficked online. In the United Kingdom, more than 8,500 sexual services ads are posted online every month . . . . The Philippines Department of Justice receives over 3,000 each month of children being sexually exploited and sold online.[101]

In a speech to the 2019 Alliance Against Trafficking in Persons Conference, U.S. Ambassador to the Organization for Security and Cooperation in Europe (OSCE), John Richmond, noted the interwoven nature of this crime with the Internet and reminded the conference:

> "[T]rafficking in persons" does not require the movement of people across a border or even internally within a country. Trafficking is a crime of coercion not a crime of transportation.[102]

---

[99] UDHR, *supra* note 17, at art. 4.

[100] Erin I. Kunze, *Sex Trafficking Via the Internet: How International Agreements Address the Problem and Fail to Go Far Enough*, 10 J. High Tech. L. 241, 243 (2010).

[101] *The Role of Technology on Facilitating and Addressing Sex Trafficking*, EQUALITY NOW (May 22, 2019), https://web.archive.org/web/20190723185011/https://www.equalitynow.org/vienna_may2019 [https://perma.cc/4ZCA-K8HS].

[102] John Richmond, *Taking a Lesson From Traffickers: Harnessing Technology To Further the Anti-Trafficking Movement's Principal Goals*, U.S. MISSION TO THE OSCE (Apr. 8, 2019), https://osce.usmission.gov/taking-a-lesson-from-traffickers-harnessing-technology-to-further-the-anti-trafficking-movement/ [https://perma.cc/6TE3-MYQH].

The coercion—whether by recruitment via Facebook or other platforms or retention via threatened release to family members of sexually explicit compromising material—happens online. While slavery in the form of sex trafficking is the real-world manifestation of this Internet human right's infringement, the digital component exists in the recruitment and retention of the slave—effectively serving as the digitally coercive chain, first attaching to and then holding the victim in place.

Infringement of this Internet human right has been recognized at the international level via the U.N.'s Palermo Protocol on Human Trafficking, which, while adopted in 2000—well before the pervasiveness of the Internet—contains enough elasticity in Article 9's prevention language to permit states to regulate technology in order to prevent trafficking and effectuate this right.[103] Technology is, in fact, being utilized by law enforcement to detect trafficked persons (victims) and to discover and track online grooming behaviors (by perpetrators).[104]

Ideally, national legislation will take into account the indispensable online component of this crime. In the U.S., after multiple unsuccessful attempts by prosecutors in the judiciary to hold commonly used online platforms such as Backpage responsible for human trafficking,[105] Congress responded statutorily by passing the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA).[106] FOSTA amends the Communications Act of 1934 to create an exception for sex trafficking, making it easier to target websites with legal action for enabling such crimes, provides new legal recourse for victims and law enforcement alike, and imposes liability for third-party content on websites that "unlawfully promote or facilitate prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims."[107] FOSTA narrows the scope

---

[103] Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, at art. 9, Nov. 15, 2000, 2237 U.N.T.S.

[104] Richmond, *supra* note 102.

[105] Sona Movsisyan, *Human Trafficking in a Digital Age: Who Should Be Held Accountable?*, 27 MICH. STATE INT'L L. REV. 540, 554–556 (2019); *See, e*.g., M.A. ex rel. P.K. v. Vill. Voice Media Holdings, LCC, 809 F. Supp. 2d 1041, 1058 (E.D. Mo. 2011).

[106] 18 U.S.C.A. § 2421A (2018).

[107] Allow States and Victims to Fight Online Sex Trafficking Act , Pub. L. No. 115-164, 132 Stat. 1253; *By Signing the Allow States and Victims to Fight Online Sex Trafficking Act, President Donald J. Trump Provides Invaluable Tools Needed to Fight the Scourge of Sex Trafficking*, THE WHITE HOUSE (Apr. 11, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/signing-allow-states-victims-fight-online-sex-trafficking-act-president-donald-j-trump-provides-invaluable-tools-

of immunity given by Section 230 and expressly provides that Section 230 has "[n]o effect on sex trafficking law."[108]

In the European Union, Directive 2011/36 provides the operative regulatory framework and requires Members States to report on their efforts to the E.U. Anti-Trafficking Coordinator.[109] Pursuant to this law, the European Commission reports bi-annually on progress toward combatting human trafficking and, as stated in its 2018 report that while Internet recruitment remains strong, the levels of state investigation and prosecution remain low, thereby lowering the risk faced by perpetrators—especially in E.U. countries where prostitution is legal.[110] Thus, a more comprehensive strategy was recommended.[111]

That conclusion can be taken as a macro-statement for both national and international efforts to combat this conduct and thereby effectuate this human right. Technology must be part of the solution, but as noted above, developments are just now beginning on this front. However, absent the comprehensive strategies, freedom from slavery as an Internet human right remains only recognized but not effectively secured at this point.

Article 5: Freedom from Torture and Degrading Treatment

The UDHR's prohibition on torture and degrading treatment appears in Article 5, which states:

> No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment.[112]

---

needed-fight-scourge-sex-trafficking/?utm_source=link&utm_medium=header [https://perma.cc/N792-SPJA].

[108] *J.B. v. G6 Hosp., LLC*, No. 19-cv-07848-HSG, 2020 WL 4901196, at *4 (N.D. Cal. 2020); 18 U.S.C.A. § 2421A (2018).

[109] Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on Preventing and Combating Trafficking in Human Beings and Protecting Its Victims, and Replacing Council Framework Decision 2002/629/JHA, O.J. (L 101) 1, 5 (April 15, 2011).

[110] *Rep. From The Commission to the European Parliament and the Council, Second Report On The Progress Made In The Fight Against Trafficking In Human Beings (2018) As Required Under Article 20 Of Directive 2011/36/EU On Preventing And Combating Trafficking In Human Beings And Protecting Its Victims*, at 3, 5, 7 COM (2018) 777 final (March 12, 2018).

[111] *Id.*

[112] UDHR, *supra* note 17, at art. 5.

Translated to the cyber-context, the degrading treatment protected against would not be physical but rather psychological torture—specifically cyber-bullying. Although there is no universally agreed definition of cyber-bullying, there are common features that make it stand out from other online attacks such as harassment: "[C]yberbullying . . . is generally considered to include conduct resulting in 'willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices.'"[113]

The conversion of this human right to digital form narrows its scope, capturing only the treatment aspect but not the punishment aspect, focusing on the "cruel, inhuman or degrading" component, but not torture. International legal definitions of torture typically entail both a coercive motive and an official component, e.g. state action,[114] which would not be present in the cyber-context. Cyber-bullying is perpetrated by one individual or group against another, implicating neither state coercion[115] nor action.

Some have nevertheless concluded that cyber-bullying is a form of torture, even if it does not meet the elements provided in the Convention Against Torture, "CAT".[116] Both the degree of psychological torture and the dramatically increased adverse consequences lead to that conclusion.[117] Especially among teens, the risk of suicide by victims of cyber-bullying is far higher than victims of traditional bullying.[118] Key differentiators underlying this statistical gap are the anonymity of the perpetrator and the potentially much larger audience that cyber-bullying can create, neither of which exist in the traditional bullying context.[119] Moreover, the statistics are alarming: "about 1 in every 4 teens has experienced cyberbullying, and about 1 in 6 has

---

[113] Kimberly Miller, Note, *Cyberbullying and its Consequences: How Cyberbullying is Contorting the Minds of Victims and Bullies Alike, and the Law's Limited Available Redress*, 26 S. CAL. INTERDIS. L.J. 379, 380 (2017).

[114] *See, e.g.*, U.N. Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Dec. 10, 1984, 1465 U.N.T.S. 85, at art. 1, 2; *see also Torture Research Guide*, INTERNATIONAL JUSTICE RESOURCE CENTER, https://ijrcenter.org/thematic-research-guides/torture/ [https://perma.cc/7CZG-2QDW] (last visited Apr. 17, 2023) (providing the definition of torture and describing relevant enforcement and case law).

[115] Ashley Abramson, *Cyberbullying: What Is It and How Can You Stop It?*, Am. Psych. Assoc. Blog, Sep. 7, 2002.

[116] Samantha Newbery & Ali Dehghantanha, *Torture-Free Cyber Space: A Human Right*, U. of Salford (Manchester), ELSEVIER 1, 5 (2017).

[117] *Id.* at 3.

[118] *Id.*at 5.

[119] Alison V. King, *Constitutionality of Cyberbullying Laws: Keeping the Online Playground Safe for Both Teens and Free Speech*, 63 VAND. L. REV. 845, 850–51 (2010).

been a perpetrator. About 1 in 5 tweens, or kids ages 9 to 12, has been involved in cyberbullying. . . ."[120]

Article 5's protection from cruel, inhuman, or degrading treatment in the form of cyber-bullying as an Internet human right is codified by many countries and U.S. states.[121] From a regulatory approach, stripping away anonymity is thought to be one method of deterring cyber-bullies, since anonymity in some cases actually incentivizes cyberbullying, but may at the same time impact rights to freedom of expression. For example, South Africa has adopted laws to combat cyberbullying that require ISPs to hand over contact details of a harasser online, and China's approach to tackle cyberbullying includes requiring people to register their real names online, making it easier to track individuals and hold them accountable.[122]

There are a diverse array of strategies employed by countries and U.S. states to tackle cyber-bullying:

- **Canada**- Under the Education Act, individuals who engage in cyberbullying face suspension from school. Repeat bullies may also face expulsion and possible jail time.
- **United Kingdom**- Under the Malicious Communications Act, cyberbullying could result in six months or more in prison and a hefty fine.
- **Philippines**- Under Republic Act 10627, it is up to the schools to implement policies to address cyberbullying. If school administrators do not comply with the Republic Act, they face sanctions.
- **Australia**- Under the Federal Nature of Law, cyberbullying laws vary from territory to territory. The laws in each territory take three forms: Actions by state, lawsuit by the victim, and "Articulate of Industry Codes."
- **Idaho**- Under "Jared's Law," a student who engages in cyberbullying is found guilty of a misdemeanor.

---

[120] Abramson, *supra* note 14.

[121] *See Cyberbullying Enacted Legislation: 2006-2010*, NAT'L CONF. OF STATE LEGISLATURES: ISSUES & RSCH., https://web.archive.org/web/20110113042238/http://www.ncsl.org/default.aspx?tabid=12903 [https://perma.cc/WR67-6USL] (last visited Apr. 2, 2023).

[122] *A Guide to Worldwide Bullying Laws*, HENRY CARUS + ASSOCIATES, https://www.hcalawyers.com.au/blog/bullying-laws-around-the-world/ [https://perma.cc/3GY7-LS3W] (last visited Apr. 2, 2023).

- **Hawaii**- Under the SB2094 law, a student who engages in cyberbullying is fined $100 per offense.
- **Louisiana**- Under H.B.1259, Act 989, a student who engages in cyberbullying is fined $500 or imprisonment for up to six months.
- **Maryland**- Under "Grace's Law," cyberbullies are charged with a misdemeanor, a prison sentence of one year, and a $500 fine.
- **North Carolina**- Under 14-458.1, defendants who are over the age of 18 and engage in cyberbullying are charged with a class one misdemeanor. If the defendant is under the age of 18, they are charged with a class two misdemeanor.
- **Tennessee**- Under S.B.113, a student engaged in cyberbullying and online threats is punished with a misdemeanor, with up to a year imprisonment. The cyberbully also faces a $2,500 fine.
- **Wisconsin**- Under 947.0125, if a student uses computers unlawfully, they are charged with a class B misdemeanor and a fine of $1,000. They could also face a prison sentence of three months.
- **United States**- The following states have implemented cyberbullying laws that punish the cyberbully with suspension or expulsion: California, Connecticut, Colorado, and Illinois.
- In **New Jersey**, the punishment for cyberbullying ranges anywhere from detention to expulsion.
- In **Vermont,** the punishment for cyberbullying is expulsion.[123]

Much progress has been made at the state level to protect individuals from psychological torture and degrading treatment in the form of cyber-bullying, although very little has been accomplished at the international level. Cultural norms may have a dampening effect on such efforts, thereby creating uneven regulation across the Internet. Nonetheless, targeting which disproportionately affects women, children, and minorities in this area continues to drive a sense of urgency by policymakers across states which could mitigate that possibility.[124]

Article 6: Right to Recognition Before the Law

[123] Steven Woda, *Cyberbullying Laws Around the Globe: Where is Legislation Strongest?*, UKNOWKIDS (Oct. 16, 2014, 7:56 PM), https://resources.uknowkids.com/blog/cyberbullying-laws-around-the-globe-where-is-legislation-strongest [https://perma.cc/7JHH-CKRC].

[124] Francesca Gottschalk, *Cyberbullying: An Overview of Research and Policy in OECD Countries*, OECD Education Working Papers (No. 270), OECD Publishing (2022), https://doi.org/10.1787/f60b492b-en.

Focusing on legal personality, or legal existence, Article 6 provides:

> Everyone has the right to recognition everywhere as a person before the law.[125]

The obverse of this is the right to non-recognition, or anonymity. That more clearly manifests as a form of privacy right, discussed below in Article 12. However, with respect to the positive ascertainment of this right, there are three manifestations it takes: biased technology, digital inequality, and digital persona. Although there has been more activity in the last area, the first two bear mention. It should be noted, we are not exploring here issues of "legal identity," a growing field spurred by implementation of the United Nations (UN) Sustainable Development Goal (SDG) 16.9, which provides, "By 2030, provide legal identity for all, including birth registration."[126]

Unlike many of the other rights that tend to focus on an object, such as free exercise of religion or freedom from slavery, that is either objectively discernable or not, the object of Article 6, recognition before the law, is a much more subjective determination in nature. As such, it is more difficult to ascertain this article's application as an Internet human right because its migration into digital reality is tricky to pin down as it can look like many things. Furthermore, it is entirely dependent upon access, which is not uniformly available, and which raises the predicate question of whether one is entitled to an online right of recognition if one does not have access to the Internet.

---

[125] UDHR, *supra* note 17, at art. 6.

[126] *See Sustainable Development*, U.N. DEP'T OF ECON. AND SOC. AFF., https://sdgs.un.org/goals/goal16 [https://perma.cc/T5W3-TLBL] (last visited Apr. 2, 2023). Subsequent to the adoption of the SGDs, the UN' Economic and Social Council adopted the following definition of legal identity: "*…the basic characteristics of an individual's identity, for example, name, sex, and place and date of birth, conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. In the absence of birth registration, legal identity may be conferred by a legally recognized identification authority; this system should be linked to the civil registration system to ensure a holistic approach to legal identity from birth to death*…." U.N. Secretary-General, *Introduction of the United Nations Legal Identity Agenda: a Holistic Approach to Civil Registration, Vital Statistics and Identity Management*, at 3 E/CN.3/2020/15 (Dec. 18, 2019). While it is expected that systems and credentials for identity will be digital and Internet-based, the definition of "legal identity" as an Internet human right is not determinative.

Bias in the creation of technology, typically unintentional, may create gaps in recognition of the person that violates this Internet human right in two instances: when programmers fail to recognize and close those gaps or when the resulting algorithm or AI that is created but begins running on its own subsequently creates new gaps, or reinforces bias-at-the-formation that it also fails to recognize and close, or even fails to recognize that the gap *should* be closed even if it is discovers one.

The first instance occurs when technology development teams lack diversity, which can result in biased AI or tech systems. For example, prior to its release, Microsoft's Kinect gaming system for Xbox was only tested on men ages 18 to 35, which initially resulted in a system that did not recognize women or children.[127] Similarly, development teams have deployed facial recognition systems which can more easily and accurately identify light-skin males, rather than women or darker-skinned people.[128]

The second instance occurs when an algorithm creates its own gaps in recognition, perhaps unbeknownst to the programmers or the system operationally deploying the AI.[129] One of the challenges in algorithm bias is that it can grow exponentially (i.e., it reinforces biases in its initial design) and, when this growth occurs, it can have an unintended ripple effect.[130] Neutral algorithm procedures can also produce decisions that disproportionately and systematically harm protected classes.[131] For example, the U.S. Department of Housing and Urban Development brought a suit against Facebook because it used a machine-learning algorithm to select a housing advertiser's audience in a fashion that excluded certain minority groups.[132]

Solutions exist for each of these bias problems that would help ensure recognition. Increasing the diversity of both the programmers and test audiences would alleviate the first type and introducing HITL (human in the loop) processes to check feedback, impact, evolution, and application of

---

[127] Alina Tugend, *Exposing the Bias Embedded in Tech*, N.Y. TIMES (June 17, 2019), https://www.nytimes.com/2019/06/17/business/artificial-intelligence-bias-tech.html [https://perma.cc/QCB2-L9M3].
[128] *Id.*
[129] Patrick Huston & Lourdes Fuentes-Slater, *The Legal Risk of Bias in Artificial Intelligence*, LAW 360 (May 27, 2020), https://www.law360.com/articles/1274143/the-legal-risks-of-bias-in-artificial-intelligence [https://perma.cc/F3QL-ZSHC].
[130] *Id.*
[131] Mark MacCarthy, *Fairness in Algorithmic Decision-Making*, BROOKINGS (Dec. 6, 2019), https://www.brookings.edu/research/fairness-in-algorithmic-decision-making/ [https://perma.cc/7JJA-25CN].
[132] *Id.*

deployed algorithmic or AI systems would alleviate the second type—although reintroducing the human element into an automated system would to some degree defeat the purpose of moving to an automated system. Nevertheless, two bills were introduced in Congress, though not passed, that would address such issues: the Algorithmic Accountability Act of 2019 and the Commercial Facial Recognition Act of 2019.[133] Thus, recognition of the bias issue in cyberspace is beginning to coalesce.

Yet, it is the "digital persona" manifestation that perhaps most directly implicates Article 6's human right to recognition of the person. Digital personae are digital representations of individuals or a "model of an individual's public personality based on data and maintained by transactions and intended for use as a proxy for the individual."[134] Digital personae can be projected (how an individual chooses to represent themselves), imposed (created by institutions based on the information they collect about an individual), or a hybrid of the two. An example how these can evolve together arises where an individual provides curated information to create a profile page on Facebook, which is a projected persona. When Facebook combines the user information with data concerning web browsing behavior, this creates an imposed persona.[135]

Digital personae and online profiles represent real-world individuals, meaning that the use of digital personae may have a direct effect on these individuals.[136] When an individual is "unable to construct his own individual identity in a manner that is free from unreasonable constraints, and in line with his own wishes and desires, the human dignity of this individual is affected."[137] The legal personality or legal status of digital personae is still being debated. Although the rights reflected in the UDHR were clearly designed to protect living human beings, it remains unsettled whether attributing legal status to digital personae may bring protection for the personae (and, thus, indirectly for the individual).

In some ways, this logic relates to the protection of one's online avatar in a multi-player gaming environment, as discussed with respect to the freedom

---

[133] *AI Legislation Tracker—U.S.*, CENTER FOR DATA INNOVATION (Dec. 2, 2019), https://www.datainnovation.org/ai-policy-leadership/ai-legislation-tracker/ [https://perma.cc/SEE7-JJJZ]; Algorithmic Accountability Act of 2019, S. 1108, 116th Cong. (2019); Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019).

[134] ARNOLD ROOSENDAAL, DIGITAL PERSONAE AND PROFILES IN LAW: PROTECTING INDIVIDUALS' RIGHTS IN ONLINE CONTEXTS 8 (2013).

[135] *Id.* at 8.

[136] *Id.* at 8–9.

[137] *Id.* at 199.

from harassment. However, in this debate over legal personalities, a distinction is made between passive and active digital personas.[138] As VR, AR and even gaming experiences in the "metaverse" become more sophisticated and complicated, legal responses including case law and regulation will also likely accompany that evolution.

Another species of the digital persona is the "digital dossier," which differs from the original version in that another author is introduced to the creation of the digital persona. Digital dossiers are constructed through the flow in information between (1) large computer databases of private-sector companies, (2) public records, and (3) government agencies and law enforcement officials.[139] The laws of information privacy are more clearly implicated with respect to the assembly and online creation of digital dossiers. Indeed, the law actively "contributes to the creation of our dossiers by compelling people to give up personal data, placing it in public records, and then allowing it to be amassed by database companies."[140] Thus, in some ways, the digital dossier is very closely akin to the passive digital persona.[141]

Both the active and passive aspects of digital personae, and certainly in the case of digital dossiers, the individual enjoys no absolute right to control their digital persona. For example, Facebook famously divests users of exclusive rights to content they post on its digital platform.[142] The law has begun to take steps to allow individuals to protect and correct their individual digital persons. The Uniform Law Commission has proposed the Uniform Personal Data Protection Act (UPDPA), meant to protect individual data and records held by private-sector companies.[143] If adopted, the UPDPA would allow an individual to correct and remove personal data and therefore correct

---

[138] *Id.* at 199–200.

[139] DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 94 (2004).

[140] *Id.* at 3.

[141] *See generally* Roger Clarke, *The Digital Persona and Its Application to Data Surveillance*, 10 INFO. SOC'Y 77 (1994).

[142] However, there are restrictions on how Facebook itself can then use that content, much of which was put in place via a consent decree with the federal government in the wake of the Cambridge Analytica scandal. *See* David C. Vladeck, *Facebook, Cambridge Analytica, and the Regulator's Dilemma: Clueless or Venal?*, HARVARD LAW REVIEW BLOG (April 4, 2018), https://blog.harvardlawreview.org/facebook-cambridge-analytica-and-the-regulators-dilemma-clueless-or-venal/ [https://perma.cc/4VN8-BBCK].

[143] *See generally* UNIFORM LAW COMMISSION, UNIFORM PERSONAL DATA PROTECTION ACT (2021), https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=cd42cede-b04f-b58f-04c6-aa8c825a8cfa [https://perma.cc/SAA3-MU8T] (drafting proposed statutory language for an Act to regulate the processing of personal data).

and modify their digital persona.[144] Philosophically, control may not be an aspect of recognition before the law, but recognition does imply accuracy in representing who the person is, and if a person lacks control over how they are represented digitally, then such accuracy suffers and this right is implicated.

The three policy areas chiefly implicated by digital recognition embraced by the Internet version of Article 6, biased technology, digital inequality, and digital persona, are diverse in both scope and application. Consequently, eventual regulation of them will likely look quite different across this spectrum. For example, rooting out bias from AI design, deployment, and operation will have a very different regulatory footprint than according some form of legal status to digital personae necessary to ensure their protection. Thus, Article 6 exemplifies the need for varied legal approaches to distinct Internet-based issues that must be addressed for it to be said that this particular human right has achieved digital reality. In other words, the splintering of a human right from the physical world into multiple aspects once in cyberspace is a real possibility and an unavoidable component of the transference process.

Article 7: Right to Equality Before the Law

UDHR's Article 7 is a more specific, combined, extension of the general right to equality reflected in Article 1 and the general freedom from discrimination reflected in Article 2.[145] Article 7 more precisely requires these two principles be protected before the law. It provides:

> All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.[146]

While Article 7's provision of "equal protection if the law. . ." steers one perhaps towards a due process analysis, we deal with due process issues in

---

[144] *Id.*

[145] MORSINK, *supra* note 25, at 25, 59 (explaining the split between Article 2 and Article 7, which were originally a single non-discrimination article during the UDHR's negotiating process.).

[146] UDHR, *supra* note 17, at art. 7.

the discussion of Articles 8-11, below. Instead, we look at Article 7 from the point of view of non-discriminatory access to the Internet.

The operative question in this case is under *which* law are people entitled to equal protection? Because the enforcement of such rights will be at the national level, this raises a jurisdictional question. For example, Internet rights afforded to users in one country may be different from the rights of users in another country. Under different approaches to Internet regulation, which protections (if any) should be granted?

Because this is an Internet human right predicated upon how users interact with the law, state action is implicated. The most common form of state action impeding this right, then, would be temporary government shut-down of Internet service—either completely or with respect to targeted populations. Thus, the right implicated in cyberspace would be uninterrupted connectivity by of avoiding government shutdowns, typically by switching to alternate technology platforms.

Governments often have the option to execute only partial, targeted shutdown, instead of complete shutdowns. For example, in October 2016, Turkey shut down the Internet in 11 Kurdish cities across southeastern Turkey after protests broke out in response to the detention of local Kurdish officials by Turkish authorities.[147] "As much as 8% of Turkey's entire infrastructure ha[d] been rendered unreachable and affected around six million people."[148]

A report by the Brookings Institution counted 35 such government-controlled Internet shutdowns in a sampling window between January 2015 and November 2016.[149] Similarly, under the discrimination prong, governments could violate this right by blocking access to certain Internet content or certain websites. For example, Russia and Kazakhstan have laws that permit blocking "extremist" websites without any judicial oversights, and it is in the discretion of the government as to what is considered "extremist."[150] Tracking usage is another way to build a datapoint that the

---

[147] India Ashok, *Turkey Uses Emergency Decree to Shut Down Internet in 11 Kurdish Cities Amid Widespread Protests*, INT'L BUS. TIMES (Oct. 28, 2016), https://www.ibtimes.co.uk/turkey-uses-emergency-decree-shut-down-internet-11-kurdish-cities-amid-widespread-protests-1588701 [https://perma.cc/5X6Y-CXL4].

[148] *Id.*

[149] Catherine Howell and Darrell West, *The Internet as a Human Right*, BROOKINGS (Nov. 7, 2016), https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/ [https://perma.cc/6N8F-2Q5K].

[150] Nancy Scola, *In the 'Global Struggle for Internet Freedom,' the Internet is Losing, Report Finds*, WASH. POST (Dec. 4, 2014), https://www.washingtonpost.com/news/the-

government can then use to target shut-downs; for instance, Nigeria has a law requiring Internet cafes to keep logs of customers who come into their shops and use their computers.[151]

For purposes of Article 7, attempted control by "Big Tech" companies or by individuals would not qualify due to the nexus with "the law." In fact, in the United States, Big Tech is commonly protected from legal action regarding policing of content on their platforms. For example, Section 230 of the Communications Decency Act of 1996 in the United States shields ISPs, social media sites, and streaming services from lawsuits over content provided by others,[152] although the Justice Department has recently proposed rolling back some of these protections in order to induce more active policing by these companies.[153]

That said, it is not so clear when the controller or the object of the control is a government official using a private platform. A U.S. federal court ruled that President Trump could not block critics from his Twitter account under the First Amendment.[154] The social media accounts of public officials are "now among the most significant forums for discussion of government policy."[155] Although the blocking feature is available to all Twitter uses, President Trump's use of blocking of certain followers was unacceptable because the president's Twitter account is "one of the White House's main vehicles for conducting official business."[156] Nevertheless, Twitter began

switch/wp/2014/12/04/in-the-global-struggle-for-internet-freedom-the-internet-is-losing-report-finds/ [https://perma.cc/GE24-97LY].

[151] *Id.*

[152] Brent Kendall and John McKinnon, *Justice Department Proposes Limiting Internet Companies' Protections*, WALL STREET J. (June 17, 2020), https://www.wsj.com/articles/justice-department-to-propose-limiting-internet-firms-protections-11592391602 [https://perma.cc/97G8-ZLCF].

[153] Jacob Gershman, *The Defining Law of the Internet Age*, WALL STREET J. (June 17, 2020), https://www.wsj.com/articles/the-defining-law-of-the-internet-age-11592412911 [https://perma.cc/22YT-9BXE].

[154] Vanessa Romo, *U.S. Appeals Court Rules Trump Violated 1st Amendment By Blocking Twitter Followers*, NPR (July 9, 2019), https://www.npr.org/2019/07/09/739906562/u-s-appeals-court-rules-trump-violated-first-amendment-by-blocking-twitter-follo [https://perma.cc/59EV-ANKD].

[155] *Id.*

[156] *Id.*

labeling President Trump's tweets as "manipulated media"[157] and Facebook removed a Trump ad containing a widely acknowledged hate symbol.[158]

Some countries have turned their efforts to protecting Internet rights, pledging to avoid shutdowns, such as Brazil, which passed its Marco Civil da Internet ("Internet Bill of Rights") that includes net neutrality and privacy protections, and India, which relaxed a rule on Internet access and content that had been put into place following riots a year prior.[159] However, technology itself may be the best recourse against repressive regimes bent on temporarily shutting down the Internet or parts thereof.

Internet activists have figured out creative ways around restrictions. Greatfire, for instance, provides a service that takes online content blocked in China and hosts it on global platforms (like Amazon servers). This makes it difficult for the Chinese government to block the content, both politically and technologically. Workarounds such as this have kept widespread political protests going in Hong Kong[160] and Iran[161] when the government seeks to disrupt Internet-based communications among protestors (thereby disrupting the movement) and between protestors and the outside world (thereby muzzling their message to the world community).[162]

Consequently, Article 7's transformation into an Internet human right to freedom from temporary government shutdown of service is becoming recognized but exists too close to what many authoritarian governments consider to be their internal sovereign power to maintain order. As a result, challenges to such order, especially political ones, are unlikely to be successful in effectuating this human right. International action will be needed in this regard.

Article 8: Right to Remedy

---

[157] *Twitter Labels Trump Tweet 'Manipulated Media' For First Time*, BBC (June 19, 2020), https://www.bbc.com/news/technology-53106029 **[**https://perma.cc/EK7H-RY9L**].**

[158] *Facebook Removes Trump Ad Over 'Nazi Hate Symbol'*, BBC (June 18, 2020), https://www.bbc.com/news/world-us-canada-53098439 **[**https://perma.cc/HZB2-4UTM].

[159] Scola, *supra* note 150.

[160] Matthew De Silva, *Hong Kong Protestors Are Once Again Using Mesh Networks To Preempt An Internet Shutdown*, QUARTZ (Sep. 3, 2019), https://qz.com/1701045/hong-kong-protestors-use-bridgefy-to-preempt-internet-shutdown [https://perma.cc/74BW-M7T6].

[161] Mehr Nadeem, *How the Iranian Diaspora is Using Old-School Tech to Fight Internet Shutdown at Home*, REST OF WORLD (Sep. 24, 2020), https://restofworld.org/2020/cat-and-mouse-censorship/ [https://perma.cc/QM49-CQS9].

[162] Ivana Kottasová and Sara Mazloumsaki, *The 'Internet As We Know It' Is Off In Iran. Here's Why This Shutdown Is Different*, CNN (Nov. 19, 2019), https://www.wral.com/the-internet-as-we-know-it-is-off-in-iran-heres-why-this-shutdown-is-different/18778492/?version=amp [https://perma.cc/45ZZ-QNEH].

What is a right without a remedy? Chief Justice John Marshall observed in *Marbury v. Madison*,[163] "The government of the United States has been emphatically termed a government of laws, and not of men. It will certainly cease to deserve this high appellation, if the laws furnish no remedy for the violation of a vested legal right."[164] There are two parts, then to the analysis of UDHR Article 8's promise:

> Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law.[165]

In this case, it is the Council of Europe that provides clear guidance. It states that "individuals have the right to an effective remedy when human rights are restricted or violated."[166] A remedy is not always tied to legal action, but the Council notes whatever the avenue for seeking a remedy, the remedy should be accessible and affordable.[167] Moreover, remedy types are as varied as the claims. The Council cites the following examples of effective remedies: inquiry, explanation, reply, correction, apology, reinstatement, reconnection, and compensation.[168]

In the digital realm, under the Council of Europe's guidance, both ISP's and Member State governments can also be obligated to provide such remedies. For example, Internet service providers have an obligation to inform users about their rights, freedoms, remedies, and how to obtain them. For instance, Google Search's European branch contains information in a readily accessible format on their FAQ page about how to petition Google to take down information according to their rights under Article 12.[169] Internet

---

[163] Marbury v. Madison, 5 U.S. 137 (1803).
[164] *Id.* at 163.
[165] UDHR, *supra* note 17, at art. 8.
[166] *Guide to Human Rights for Internet Users, Recommendation CM/Rec (2014)6 and explanatory memorandum*, COUNCIL OF EUR. 6 (2014), https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2014-6-of-the-committee-of-ministers-to-member-states-on-a-guide-to-human-rights-for-Internet-users-adopted-by-the-committee-of- [https://perma.cc/P5AC-SG5B].
[167] *Id.* at 6.
[168] *Id.*
[169] *Right to Be Forgotten Overview*, Google, https://support.google.com/legal/answer/10769224?hl=en (last visited April 25, 2023).

users should have effective remedies against measures of internet disconnection, including the ISP informing users about the grounds and legal basis for disconnection measures. National authorities have an obligation to protect people from criminal activity or criminal offenses committed on or by using the Internet.[170]

However, with respect to deputizing private corporations as both the forum to hear remedy claims and to grant or deny remedies, a special rapporteur for the International Law Commission said, "Complex questions of fact and law should generally be adjudicated by public institutions, not private actors whose current processes may be inconsistent with due process standards and whose motives are principally economic."[171] This observation poses an interesting policy question about private companies monitoring or policing content. Facebook and Twitter are not "competent national tribunal[s]" so to what extent do they have the power to make determinations about potential human rights violations or remedies? Similarly, when Google decides to delist content, it is still answerable to the Data Protection Authority if that content should be delisted but was not. However, there is no protection going the other way—when information is delisted but should not have been. While it is no more a "competent tribunal" than Facebook or Twitter, Google in this case acts as a court, but without any of the public oversight a court would face.

Nevertheless, Facebook has created what some are referring to as a "Supreme Court" of up to 40 outside individuals to hear appeals from users whose content has been removed from the platform and make a recommendation to the company.[172] The draft bylaws lay out a straightforward process, albeit one that may call upon users to assemble more information than perhaps a reasonable user is capable of assembling—such as the extent to which other users are harmed by the removal of the original post. [173]

Likewise, YouTube has created a video removal and appeals process that has resulted in an overwhelming denial rate, "YouTube's latest transparency report suggests its appeals process is failing creators. Last quarter, YouTube

---

[170] *Id.* at 13.

[171] Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Int'l Law Comm'n, U.N. Doc. A/HRC/38/35 (Apr. 6, 2018).

[172] Jessica Guynn, *This Is How You Will Appeal to Facebook's 'Supreme Court' When Your Post Is Taken Down*, USA TODAY (Jan. 28, 2020, 2:00 PM), https://www.usatoday.com/story/tech/2020/01/28/facebook-and-instagram-how-you-can-appeal-when-your-post-removed/4593405002/ [https://perma.cc/QD6Y-FC9C] (explaining the process for appealing content removal under Facebook's 2020 proposed rules).

[173] *See id.* (detailing the requirements laid out by Facebook's proposed appeals process).

removed 5.9 million videos from the platform. It received just 108,779 appeals, but it only reinstated 23,471 of those videos. That means roughly 78 percent of appeals were rejected."[174] Users have called for an overhaul of the process and placing it under the control of an outside third party. "While cleaning up the platform is a good thing, the fact that YouTube shoots down the vast majority of appeals is not -- especially if you're a creator who relies on the platform as a source of income."[175]

Consequently, remedies stemming from states for infringement of Internet human rights are going to look quite different from those stemming from companies. On the state side, full or partial government shutdown of Internet access by authoritarian regimes during periods of political and social unrest or perceived national security threats is a main driver violating this promise. On the company side, remedies may exist within relevant terms of service for users of particular platforms; however, these may prove inadequate or unsatisfactorily address the rights violation at hand. In extreme cases, courts may step in to mandate further remedies, such as in the case of Google being ordered to design and operate a right to be forgotten within the E.U.,[176] but this possibility remains the exception rather than the rule.

Article 9: Freedom from Arbitrary Detention

Designed to prohibit holding or banishing people against their will, UDHR's Article 9 states:

> No one shall be subjected to arbitrary arrest, detention or exile.[177]

In the absence of any known case law or official interpretation of what exile means in the context of Article 9, averring that "exile" may be the equivalent of being banned from a site or app and recognizing that in the United States such banishment has usually been approached from a freedom of expression context (discussed elsewhere), in the context of Internet human

---

[174] Christine Fisher, *Youtube's Appeal Process is Largely Ineffective*, ENGADGET (Feb. 28, 2020, 4:10 PM), https://www.engadget.com/2020-02-28-youtube-video-removal-appeal-process.html [https://perma.cc/H5DS-DFBY].
[175] *Id.*
[176] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN [http://perma.cc/ED5L-DZRK].
[177] UDHR, *supra* note 17, at art. 9.

rights, Article 9 could take on at least two forms, (1) digital exile from social media and other platforms, and (2) Internet access rights for individuals who are incarcerated. Thus, while the real-world analogues of arrest and detention do not easily translate to the digital world, the exile component, or "lock out," does.

Being banned from an Internet site, like being banned from a commercial establishment in a town or city, is typically the decision of the proprietor. Although there are certain constraints on banning people from commercial establishments in the physical world, such as protections against racial discrimination, it is unclear if such constraints exist in the realm of the Internet or whether such a proprietor would even know the race of the person being banned in order to trigger such constraints.

Digital exile can occur in a purely commercial setting that is transactional in nature, such as being banned from a hotel website,[178] but it occurs much more frequently in the social media setting. In that setting, those whose accounts are deactivated by Facebook[179] or Instagram[180] are typically done in response to repeated postings by the individual which violate the terms of service they agreed to when joining the platform. In that respect, the person is both on notice and in breach of an agreement; thus, recourse to oppose digital exile may be considered waived in some instances.

Social media companies establish levels of enforcement, however, before finally arriving at digital exile. For example, Twitter may take enforcement actions at the "tweet-level," direct message level, or account level, depending upon the type of violative posting involved and whether the poster is a repeat offender despite receiving notices to cease making similar posts.[181]

---

[178] Jackson Cunningham, *Digital Exile: How I Got Banned for Life from AirBnB*, MEDIUM (July 3, 2018), https://jacksoncunningham.medium.com/digital-exile-how-i-got-banned-for-life-from-airbnb-615434c6eeba [https://perma.cc/Z2UT-R87Y] (providing an anecdote of commercial digital exile).

[179] *See Disabling Accounts*, META (Jan. 19, 2022), https://transparency.fb.com/enforcement/taking-action/disabling-accounts/ [https://perma.cc/2RGK-TKD5] (detailing Facebook policy for disabling accounts); *See also* Leonid Bershidsky, *Banned from Facebook? A Polish Court May Help*, BLOOMBERG (May 9, 2019, 7:27 AM), https://www.bloomberg.com/opinion/articles/2019-05-09/banned-from-facebook-a-polish-court-may-help [https://perma.cc/E497-CVCE] (explaining violation of community standards as a basis for account removal).

[180] *See* Rafael Broshi, *What to do if your Instagram account gets suspended*, NOTCH BLOG, https://www.get-notch.com/blog/what-to-do-if-your-instagram-account-gets-suspended [https://perma.cc/9723-CUBP] (last visited Apr. 8, 2023) (explaining violation of terms as a reason an account might be suspended).

[181] *Rules and Policies: Our Range of Enforcement Options*, TWITTER HELP CENTER, https://help.twitter.com/en/rules-and-policies/enforcement-options [https://perma.cc/2J2M-

Furthermore, Instagram and TikTok will institute "shadow bans" on individual accounts whose posts violate terms of service, where the user's content is hidden from other users, or the functionality somehow restricted—without the user's knowledge.[182]

While targeted threats and abusive content are grounds for exile from Twitter,[183] misuse of a platform to spread lies, conspiracy theories, and propaganda during political campaigns has led to such bans as well. During the 2020 U.S. presidential election, Twitter deactivated more than 7,000 accounts and limited 150,000 others that were run by or associated with the extreme right-wing QAnon political conspiracy group.[184] The deactivated accounts were enforced against on the basis of platform manipulation, spamming, or ban evasion.[185]

Unlike digital exile, which is the result of corporate decision-making, the issue of inmate access to the Internet implicates state rather than private action. In some countries, those who are incarcerated by the state are often not accorded certain rights during the period of their incarceration. For example, the right to bear arms or the right to privacy[186]—rights which are irreconcilable with their incarceration—may be limited. Other rights, such as voting rights, can be continued or suspended for inmates while in prison and restored upon completion of sentence, depending upon the jurisdiction.[187] Conversely, procedural due process rights[188] and protections against cruel

---

WXP6] (last visited Jan. 4, 2021) (outlining Twitter's enforcement policies in response to violation of terms of service).

[182] *See* Monique Thomas, *Does Instagram Shadowban Accounts*, LATER (June 8, 2021), https://later.com/blog/instagram-shadowban/ [https://perma.cc/LBB7-3LBK] (explaining Shadowbans with the caveat that the practice has yet to be confirmed by Instagram).

[183] *See* Alina Selyukh, *What Does It Take To Get Banned From Twitter?*, NPR (July 20, 2016, 2:31 PM), https://www.npr.org/sections/alltechconsidered/2016/07/20/486738705/what-does-it-take-to-get-permanently-banned-from-twitter [https://perma.cc/78KX-Y3D9] (describing the reasons users have been banned from Twitter).

[184] Ben Collins & Brandy Zadrozny, *Twitter Bans 7,000 Qanon Accounts, Limits 150,000 Others as Part of Broad Crackdown*, NBC (July 21, 2020, 7:59 PM), https://www.nbcnews.com/tech/tech-news/twitter-bans-7-000-qanon-accounts-limits-150-000-others-n1234541 [https://perma.cc/M9DL-U8KJ].

[185] *Id.*

[186] Hudson v. Palmer, 468 U.S. 517, 526 (1984).

[187] *See* NATIONAL CONFERENCE OF STATE LEGISLATURES, RESTORATION OF VOTING RIGHTS FOR FELONS (updated Apr. 6, 2023).

[188] *See* Wolff v. McDonnell, 418 U.S. 539, 558 (1974) (arguing "the touch stone of due process is protection of the individual against arbitrary action of the government…" and that

and unusual punishment[189] continue to be guaranteed for inmates serving their sentences.

Whether and to what extent inmates should be allowed Internet access while in prison is an unsettled question laden with many policy considerations. For example, should inmates convicted of cybercrimes then be allowed back onto a computer while in jail? Is this the equivalent of returning the weapon used to commit the crime to the perpetrator? Ultimately, the decision on whether to grant Internet access to in-mates rests with each state in the absence of an international norm. Germany, Belgium, Australia, Great Britain, and the United States have all studied the issue.

In Belgium, authorities have deployed a technological innovation known as PrisonCloud that enables inmates to access the Internet, surf the web to approved sites, watch films, play video games, and make calls.[190] This has not sat well with many in Belgian society, who liken incarceration in facilities with PrisonCloud such as Breven, outside Antwerp, to staying at a hotel.[191] One particularly upsetting fact for some is that inmates can actually view pornographic films if they pay to view.[192]

In the UnitedStates, advocates of allowing inmates Internet access argue that "Whether that right should extend to prisoners should settle not on the effectiveness of prison as punishment but on the public good it could generate for society," noting that greater access could help ameliorate the revolving door phenomenon—wherein 2/3 of released prisoners end up back in prison within three years of release.[193] This phenomenon they say, is especially true

---

"the minimum requirements of procedural due process appropriate for the circumstance must be observed").

[189] *See* Estelle v. Gamble, 429 U.S. 97, 102 (1976) (explaining "the history of the constitutional prohibition of 'cruel and unusual punishments' has been recounted at length in prior opinions of the Court…"); Gregg v. Georgia, 428 U.S. 153, 173 (1976) (extending protection against "unnecessary or wanton infliction of pain"); Helling v. McKinney, 509 U.S. 25, 31 (1993) (bringing prisoner treatment and prison conditions under 8th Amendment scrutiny); *But cf.* Sara L. Rose, *Cruel and Unusual Punishment Need Not Be Cruel, Unusual, or Punishment*, 24 CAP. U. L. REV. 827, 827-828 (1995)) (explaining the Court's initial expansion and continued revisions of the scope of Cruel and Unusual Punishment through its application to internal prison conditions).

[190] Siobhann Tighe, *Prisoners Allowed Access to Adult Films and Internet*, BBC (Apr. 22, 2016), (https://www.bbc.com/news/world-europe-36067653) [https://perma.cc/SDB5-MGUS].

[191] *Id.*

[192] *Id.*

[193] Ben Branstetter, *The Case for Internet Access in Prisons*, WASH. POST (Feb. 9, 2015, 10:40 AM), (https://www.washingtonpost.com/news/the-intersect/wp/2015/02/09/the-case-for-internet-access-in-prisons/) [https://perma.cc/H7M4-PJCZ] (arguing that internet access

when phone and Internet use has become such an integral part of daily modern life.[194] Greater access is also encouraged for greater development, gaining more education, and remaining connected with family.[195] "Aside from limited connections at a handful of juvenile detention facilities, there's no way for America's 2.3 million inmates to access the internet."[196]

With Article 9, we see once again a blend of private and public regulatory approaches to digital exile and Internet access by incarcerated individuals. Digital exile is the result of a tech company like a social media platform deciding that someone should either be temporarily suspended or permanent banned from the area it controls in cyberspace. The notice aspect of due process may be fulfilled in the company's terms of service, but the hearing aspect may or may not meaningfully occur before the individual is suspended. Similarly, reinstatement may occur rather arbitrarily, with little to no procedure. Internet rights of the incarcerated, in the form of state-controlled access, while more regularized, are still developing. Both areas of regulation and enforcement have quite a way to go before Article 9's vision can be digitally realized.

Article 10: Right to a Fair Trial

With a focus on impartial process, according to UDHR's Article 10:

> Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him.[197]

---

and computer-based technical skills are critical to future employability of prisoners after release).

[194] Peter Scharff Smith, *Imprisonment and Internet-access: Human Rights, the Principle of Normalization and the Question of Prisoners Access to Digital Communications Technology*, 30 NORDIC J. HUM. RTS. 454, 454 (2012) (arguing the internet is "almost a requirement for people who want to actively participate in some of the basic aspects of living involving education, work, and social communication").

[195] Dan Tynan, *Online Behind Bars: If Internet Access Is A Human Right, Should Prisoners Have It*?, THE GUARDIAN (Oct. 3, 2016, 6:00 AM), https://www.theguardian.com/us-news/2016/oct/03/prison-internet-access-tablets-edovo-jpay [https://perma.cc/YNX3-HPKG] (describing the difficulty inmates have connecting to the outside world without access to the internet).

[196] *Id.*

[197] UDHR, *supra* note 17, at art. 10.

While a full examination of legal issues around cybercrime is beyond the scope of this article[198], protecting human rights (including due process under law, privacy and freedom of expression) in the face of combatting cybercrime is used here as a prime example of the expression of rights in Article 10, Although the evidence might be different, aggregated from digital forensics, cyber-crime charges are typically treated as regular crimes, prosecuted according to the same standards and in the same courts as other crimes, and afforded the same fair trial and procedural guarantees. Cybercrimes generally fall into the following categories, as set forth in the Budapest Convention:[199]

- illegal access[200]
- illegal interception of data[201]
- data interference[202]
- system interference[203]
- misuse of devices[204]
- computer-related forgery[205]
- computer-related fraud[206]
- child pornography[207]
- IPR infringement[208]
- aiding and abetting[209]

[198] For a general introduction to the range of legal issues around cybercrime see WORLD BANK, *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*, World Bank (2017), www.combattingcybercrime.org) [https://perma.cc/P5KX-FEKF] [hereinafter Toolkit] (describing the Toolkits aim of capacity building to "combat cybercrime…by providing a synthesis of good practices…").
[199] Convention on Cybercrime, Budapest, Ch. 2, § 1, Nov. 23, 2001, E.T.S. 185.
[200] *Id*. at § 1, art. 2 (defining criminal illegal access as "the access to the whole or any part of a computer system without right" with the potential for Parties to include additional requirements of intent).
[201] *Id.* at art. 3.
[202] *Id.* at art. 4.
[203] *Id.* at art. 5.
[204] *Id.* at art. 6.
[205] *Id.* at art. 7.
[206] *Id.* at art. 8.
[207] *Id.* at art. 9.
[208] *Id.* at art. 10.
[209] *Id.* at art. 11.

Translated into the jargon of criminal law and procedure, these criminalized activities and conduct are sometimes more commonly referred to as follows:[210]

- Phishing/Spoofing (defined as unlawfully accessing a computer without authorization; this includes federally outlawed spam)
- Blackmail/Extortion (including the use of ransomware)
- Hacking/Accessing Stored Communications
- Non-Delivery of Merchandise (devising a scheme to defraud using the Internet)
- Electronic Harassment (including cyberbullying in some states)
- Prostitution
- Drug Trafficking
- Identity Theft
- Business E-Mail Compromise (BEC)
- Online Predators
- Human Trafficking
- Hate speech

In the U.S. federal government, the Department of Justice has a special Computer Crime & Intellectual Property Section, which, according to its mission:

> [P]revents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts. Section attorneys work to improve the domestic and international infrastructure-legal, technological, and operational—to pursue network criminals most effectively.[211]

---

[210] *See* Stephen Nale, *The 10 Most Common Internet Crimes*, COMPLEX (Nov. 14, 2012), https://www.complex.com/pop-culture/2012/11/the-10-most-common-internet-crimes/ [https://perma.cc/3YEL-F3FS]; *see also What We Investigate: Cyber Crime*, FBI, https://www.fbi.gov/investigate/cyber [https://perma.cc/CYB2-7W7R] (last visited April. 7, 2023).

[211] *United States Department of Justice Computer Crime & Intellectual Property Section*, ORGANIZATION OF AMERICAN STATES (https://www.oas.org/juridico/spanish/cyber/cyb1_ccips.pdf) [https://perma.cc/X5LV-Q6W9] (last visited Jan. 5, 2020).

Many U.S. states[212] and other countries also have their own cybercrime law enforcement units.[213]

Because cybercrime is often not contained to one jurisdiction—a single instance can travel the world over, targeting victims in other countries—global efforts have begun to study the problem and coordinate better responses which would eventually lead to investigation and prosecution under the fair trial standards contemplated in Article 10. However, these efforts have been hampered by inadequate data collection and outdated methods of investigatory and prosecutorial coordination across jurisdictions.[214] A U.N. study found that most of the nearly 70 U.N. Member States surveyed were not able to provide cybercrime enforcement statistics.[215] Only six of the countries, mostly in Europe, were able to calculate the average number of persons brought into formal contact with law enforcement authorities per recorded offences related to illegal access and computer-related fraud and forgery.[216]

Yet another aspect of ensuring Article 10's contemplated fair trial for accused cyber criminals as an Internet human right is the reliable chain of custody involved in the collecting the digital evidence needed for such a trial.[217] Once collected, the digital evidence must then undergo judicial scrutiny to determine admissibility in furtherance of a fair trial. While courts

---

[212] Steve Morgan, *Directory of U.S. State and Local Cybercrime Law Enforcement*, CYBERCRIME MAGAZINE (Oct. 25, 2022), https://cybersecurityventures.com/directory-of-u-s-state-and-local-cybercrime-law-enforcement/ [https://perma.cc/W6DU-2BJU].

[213] Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 6 UCLA J.L. & TECH. 1 (2002).

[214] *See*, Toolkit, *supra* note 198, at 199 (noting cybercrime's rapid evolution and opining that "[m]any of the existing instruments may need modification or renewal.").

[215] Allison Peters & Amy Jordan, *Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime*, 10 J. NAT'L SEC. L. & POL'Y 487, 492 (2020).

[216] *Id.* at 492–93.

[217] *See E4J University Module Series: Cybercrime*, *Module*, UNITED NATIONS OFF. ON DRUGS AND CRIME (Mar. 2019), https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html [https://perma.cc/C7GQ-T2C3] (stating that "a chain of custody must be maintained" when collecting digital evidence). In addition, the Council of Europe has opened for signature a Second Protocol to the Budapest Convention on "enhanced co-operation and disclosure of electronic evidence." *See Second Additional Protocol to the Cybercrime Convention on Enhanced Co-Operation and Disclosure of Electronic Evidence (CETS No. 224)*, COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/second-additional-protocol [https://perma.cc/8MVR-U7BB]; *see also* Toolkit, *supra* note 198, at 176.

in western industrialized democracies have well-developed systems to consider admissibility, many other countries do not.[218]

Thus, a "Harmonized Model for Digital Evidence Admissibility Assessment" has been developed to help fill this gap globally.[219] A court can utilize this model in three phases: phase one determines legality of digital evidence seized (compliance with search and seizure rules) and forensic relevance (does the digital evidence link the perpetrator with the crime?); phase two assesses the integrity of the digital evidence and weighs the credibility of expert witnesses and the quality of assessment by digital forensics labs; and phase three determines admissibility once the reliability of the evidence is established.[220] Justice systems utilizing such adapted techniques should be able to wed those to existing fair trial standards in their countries to effectuate Article 10's right to a fair trial as an Internet human right.

Such a unifying system of fair trial rights for cybercrimes holds the potential for bringing Article 10's promise into the digital realm. However, state-centric differences in approaches to criminal justice that embody divergent cultural values auger against quick resolution in this area. Moreover, although a treaty-based cybercrime effort is currently underway in the United Nations, it has yet to garner support from key sectors necessary for a consensus to move the process forward.[221] This Russian-sponsored effort, however, is widely seen to be more about altering the currently prevailing multistakeholder Internet governance paradigm and undermining human rights and less about cybercrime itself.[222] Consequently, with no credible effort on the table to replace the Budapest Convention framework,

---

[218] U.N. Security Council Counter-Terrorism Comm. Exec. Directorate, *The State of International Cooperation for Lawful Access to Digital Evidence*, CTED Trends Report, Jan. 2022, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_trends_report_lawful_access_to_digital_data_.pdf.

[219] Albert Antwi-Boasiako & Hein Venter, *Implementing the Harmonized Model for Digital Evidence Admissibility Assessment*, *in* ADVANCES IN DIGITAL FORENSICS XV, IFIP AICT 569, 19–36 (Gilbert Peterson & Sujeet Shenoi eds., 2019).

[220] *Id.* at 26–28.

[221] Justin Sherman & Mark Raymond, *The U.N. Passed a Russia-Backed Cybercrime Resolution. That's Not Good News for Internet Freedom.*, WASH. POST, Dec. 4, 2019.

[222] Deborah Brown, *Cybercrime Is Dangerous, But a New UN Treaty Could Be Worse for Rights*, JUST SECURITY, Aug. 13, 2021, https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights.

state-by-state criminalization and enforcement against the cybercrimes discussed here holds more promise in this area.

Article 11: Presumption of Innocence and Criminal Procedure

UDHR's Article 11 establishes a detailed baseline for criminal prosecutions that incorporates many general principles of criminal procedure. Specifically, it provides:

> (1) Everyone charged with a penal offence has the right to be presumed innocent until proved guilty according to law in a public trial at which he has had all the guarantees necessary for his defence. (2) No one shall be held guilty of any penal offence on account of any act or omission which did not constitute a penal offence, under national or international law, at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the penal offence was committed.[223]

Broken down, Article 11 implicates at least the following elements:

- Presumption of innocence
- Guilt proven in accordance with the law
- Public trial
- Defense rights
- No *ex post facto* application of law
- No *ex post facto* application of harsher punishment

As in the case of the fair trial provisions of Article 10, most of these safeties are already in place in most justice systems where an accused cyber criminal may find themselves prosecuted;[224] thus, their Internet human rights with respect to criminal procedure guarantees under Article 11 would be accorded as a matter of course just as in the case of a perpetrator of a non-cybercrime. The main exception that requires more exploration is the right to a presumption of innocence.

---

[223] UDHR, *supra* note 17, at art. 11.

[224] *See generally*, AMAL CLOONEY & PHILIPPA WEBB, THE RIGHT TO A FAIR TRIAL IN INTERNATIONAL LAW (2021) (suggesting that the right to a fair trial has achieved "customary status." This status has "practical implications because customary rules are binding on all states, regardless of whether they are parties to a treaty.").

While the presumption of innocence may be guaranteed by law, such presumption in the Internet age as an Internet human right can be easily turned into a widespread presumption of guilt, as media coverage now includes peoples' unfiltered opinions on social media platforms, and not only more traditional journalistic media (newspapers and television programs) that have built-in editorial control over coverage of criminal prosecutions. An Australian study of Internet impact on judicial process noted, "social media empowers anyone to be a publisher. The ability to publish is therefore readily available to people who do not have a professional background in respect of the matters about which they are communicating and whose thoughts and opinions are not fact-checked by anyone."[225] That exacerbated impact of uninformed opinion can result in what the U.K.'s former Attorney General, Dominic Grieve, has called "trial by Google."[226]

Short of doing away with juries and moving to bench trials,[227] jury training followed up with stringent jury instructions and effective contempt and enforcement procedures may be the only real way to tamp down on misuse of social media by jury members.[228] In the U.K., for instance, a juror was sentenced in the case of *A-G v. Fraill* to eight months in prison for exchanging messages on Facebook with the accused in a drug trial while she was serving on the jury in addition to searching for information about the other defendant while she was in deliberations—both actions which were violation of the judicial instructions about Internet use by jurors.[229]

Consequently, while the rest of the criminal procedure rights identified in Article 11 would normally equally exist as Internet human rights afforded

---

[225] JANE JOHNSTON ET AL., JURIS AND SOCIAL MEDIA 4 (2013), https://www.ncsc.org/__data/assets/pdf_file/0013/17230/juries-and-social-media_australia_a-wallace.pdf [https://perma.cc/3KTP-T6WA].

[226] Dominic Grieve, *Trial by Google? Juries, Social Media and the Internet*, Speech (Feb. 6, 2013), https://www.gov.uk/government/speeches/trial-by-google-juries-social-media-and-the-internet [https://perma.cc/UM3X-57XK]; *see also* Arun Rath, *The Challenge of Running Fair Trials in a Media-Saturated Age*, NPR (Mar. 8, 2015),), https://www.npr.org/2015/03/08/391708142/fair-trials-in-a-media-saturated-age [https://perma.cc/A3AB-VMYP] (discussing the difficulty of finding jurors who have not been exposed to potentially prejudicing internet content relating to the case).

[227] JAMES G. APPLE & ROBERT P. DEYLING, A PRIMER ON THE CIVIL-LAW SYSTEM 26–27 (1995) (discussing differences between common law and civil law actions, the latter of which usually do not have juries).

[228] Johnston, *supra* note 225, at 23–25.

[229] Narrelle Harris, *Social Media and the Fair Trial*, LA TROBE U., https://www.latrobe.edu.au/nest/social-media-and-the-fair-trial/ [https://perma.cc/54WE-ZMEK] (last accessed Apr. 18, 2023).

defendants in the normal course of prosecutions, and an ordinary human right afforded to defendants in non-cybercrime prosecutions, the presumption of innocence problem in the Internet age, combined with misuse of social media by juries, are problematic, although not unresolvable, features to address in fully according this right.

Article 12: Right to Privacy

The right to privacy articulated in UDHR's Article 12 is a broad one, and has served as part of the basis for modern day data protection laws.[230] While the theme of data protection is beyond the scope of this article, the authors do look at how data protection and privacy have merged as means to protect a person's on-line rights in data about them, mainly through the lens of the application of Article 12 through the exercise of the right to be forgotten. Article 12 provides:

> 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.[231]

This right received special treatment in a 2016 U.N. General Assembly resolution on the right privacy in the digital age.[232] The first clause extends the privacy protection for an individual to the family and home of that individual as well as the individual's correspondence; the second clause protects the individual against slander, libel, defamation, and misinformation. As an Internet human right, the first clause would include protection against unwarranted government surveillance, preservation of online anonymity and the "right to be forgotten;" and the second clause would include combatting online "character assassination." Article 12 has also served as the basis for modern day data protection laws.

The next aspect of Article 12's protection, online anonymity, is related to the discussion of digital personas and recognition on the Internet, but presents the obverse—i.e., is there a right *not* to be recognized online? Linking online

---

[230] *See, e.g., World Development Report 2021: Data for Better Lives*, World Bank Grp. (2021) https://www.worldbank.org/en/publication/wdr2021 [https://perma.cc/8545-R5DQ] ("Safeguards for personal data are grounded in a rights-based framework that has evolved over time . . . . These safeguards . . . were codified in international law after World War II.").
[231] UDHR, *supra* note 17, at art. 12.
[232] G.A. Res. 71/199, U.N. Doc. A/RES/71/199 at 2 (Dec. 19, 2016).

anonymity with the ability to exercise free online expression, a special rapporteur for the U.N. Human Rights Council found that encryption and anonymity are essential to securing free expression.[233] Human Rights Watch explains why this may be the case, especially in repressive societies: "Strong encryption and anonymity are critical for protecting human rights defenders, journalists, and ordinary users in the digital age . . . . Encryption allows us to preserve a safe, private space for free expression at a time when governments are expanding invasive surveillance worldwide."[234]

Akin to *maintaining* online anonymity is the effort to *achieve* it in some degree by expunging online information about oneself—otherwise known as the *right to be forgotten*. In 2014, the European Court of Justice, implementing a pair of E.U. Directives on data protection and privacy, ruled in favor of a Spanish plaintiff who had petitioned Google.es to take down decade-old searchable information about his prior conviction for real estate fraud because it was limiting his ability to work; Google refused, claiming it was not a content provider only a search engine.[235] The ECJ found that Google was in fact engaged in data processing, thereby implicating the two E.U. Directives, and so must establish a system within each of the E.U. Member States whereby individuals could petition for online material about them.[236]

Google subsequently established panels that review requests in each Member State on a case-by-case basis[237] but which focus on removal, or delisting, for requests dealing with minors, sensitive personal information, lack of public interest, and the area of criminal law exonerations, acquittals, and spent convictions.[238] As of January 2021, nearly 1 million requests have been registered to delist nearly 4 million webpages from Google's search

---

[233] David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), U.N. Doc. A/HRC/28/32 (May 22, 2015).
[234] *UN: Online Anonymity, Encryption Protect Rights*, Human Rights Watch (June 17, 2015), https://www.hrw.org/news/2015/06/17/un-online-anonymity-encryption-protect-rights [https://perma.cc/YE7W-2K43].
[235] Kelly & Satola, *supra* note 7, at 5–12.
[236] *Id.* at 7–10.
[237] *Id.* at 16–17.
[238] Google, *European Privacy Requests Search Removals*, Google Transparency Rep. Help Ctr., last visited Jan. 11, 2021.

results, with about a 50% request approval rate.[239] The sites most impacted include Facebook, Twitter, and YouTube.[240]

Most recently, the ECJ ruled in December 2022 on two questions referred by the German courts: (1) how to balance erasure rights against freedom of expression when the information returned by the search engine is allegedly inaccurate, and (2) whether thumbnail images can also be delisted.[241] The court ruled that while the burden to demonstrate "manifest inaccuracy" rests with the requester, it is up to the search engine operator to balance that request against free speech concerns; moreover, "the operator of the search engine cannot be required to investigate the facts."[242] Thus, Google can take at face value an inaccuracy based delisting request *without verifying the claim*. As to the second question, the court said yes, a thumbnail image should in principle be erased along with the underlying webpage so that searchers cannot get to the erased page via an image search.[243]

Overall, after an initial spike in the wake of the ECJ decision, delisting requests have remained relatively constant. Nevertheless, whether achieved at the outset by remaining anonymous or subsequently through the right to be forgotten, online anonymity as an expression of the Internet human right to privacy has its limits—specifically with regard to online character assassination and online defamation: libel (written defamation as in a blog post), or slander (oral defamation as via a YouTube video). Fairness as a general consideration, perhaps, calls on those who excoriate another's reputation to identify themselves, although a clear rule on this has not yet emerged in the United States.[244] Victims of online character assassination can suffer debilitating psychological trauma as a result.[245]

---

[239] *European Privacy Requests Search Removals*, GOOGLE TRANSPARENCY REP. HELP CTR., https://support.google.com/transparencyreport/answer/7347822?hl=en [https://perma.cc/64PT-FB57](last visited Jan. 11, 2021).

[240] *Id.*

[241] Persephone Bridgman Baker & Katherine Silverleaf, *Case Law, CJEU: TU, RE v. Google LLC: A Step Forward in the Rational Regulation of Data?*, INT'L FORUM FOR RESP. MEDIA BLOG (Jan. 17, 2023), https://inforrm.org/2023/01/17/case-law-eu-tu-re-v-google-llc-a-step-forward-in-the-rational-regulation-of-data-persephone-bridgman-baker-and-katherine-silverleaf/ [https://perma.cc/3FF6-7CLD].

[242] Case C-460/20, TU and RE v. Google, LLC, 2022 C.J.E.U. 15.

[243] *Id.*

[244] Michael Baumrind, *Protecting Online Anonymity and Preserving Reputation Through Due Process*, 27 GA. ST. U. L. REV. 757, 761, 799 (2012).

[245] *See* Eric Shiraev and Olga Makhovskaya, *The Traumatic Psychological Impact of Character Attacks on Targets*, *in* ROUTLEDGE HANDBOOK OF CHARACTER ASSASSINATION AND REPUTATION MANAGEMENT (Sergei A. Samoilenko, Martijn Icks, Jennifer Keohane,

In Australia, a court ordered Google to divulge "any personal details such as any names, phone numbers, location metadata and IP addressed linked to the account" of an individual who had posted a bad review of a dentist online and thereby damaged the dentist's business.[246] Google and other platforms can also face financial consequences for allowing fake reviews to damage businesses. A Dutch court in Amsterdam, for example, ordered Google to pay $1,600 to a nursery that was damaged by four fake online reviews that although identified by Google pursuant to a court order, were not removed.[247]

Online character assassination and defamation, like cybercrimes, are often not restricted to single jurisdictions—especially where the offending conduct posts to a global Internet platform; consequently, redressing such incursions against the reputation protection aspect of the Internet human right to privacy may require national courts to consider transnational issues. In 2019, an Austrian court ordered Facebook to take down a disparaging and defamatory comment in Austria about a politician in the Green Party, but the E.U. Court of Justice's Advocate General, Maciej Szpunar, said courts could order platforms like Facebook to take down their material worldwide because the European law on electronic commerce "does not regulate the territorial scope of an obligation to remove information disseminated via a social network platform . . . ."[248] This is in direct contrast to delisting under the E.U.'s right to be forgotten, where delisted URLs are only removed within the scope of Google Search's European purview.

In *Dow Jones & Co., Inc. v. Gutnick*,[249] Mr. Gutnick, a Melbourne resident sought to bring a libel suit against *Barron's* business magazine in the United States for publishing an article connecting him to money laundering operations in both the U.S and Australia.[250] The defendant argued that the correct venue was New Jersey, where the article was placed on the Internet,

---

and Erick Shiraev, eds. 2019) (discussing the direct and indirect psychological impacts of character attacks).

[246] *Google Ordered to Reveal Author of Australian Dentist's Bad Review*, BBC (Feb. 14, 2020), https://www.bbc.com/news/world-australia-51498190 [https://perma.cc/KRL2-EVCM].

[247] Kevin Rawlinson, *Google Ordered to Release Fake Reviewers' Contact Details*, BBC (March 9, 2016), https://www.bbc.com/news/technology-35764829, [https://perma.cc/Y8UM-6HSL].

[248] *EU Legal Expert Says Online Defamation Enforceable Worldwide*, AP (June 4, 2019) https://apnews.com/5ff1e6534c3944babb2a2c57a95a95b5 [https://perma.cc/9872-FLSX].

[249] *Dow Jones & Co., Inc. v Gutnick* (2002) HCA 56, (Austl.).

[250] Richard Garnett, *Dow Jones & Company Inc. v. Gutnick: An Adequate Response to Transnational Internet Defamation?*, 4 MELBOURNE J. OF INT. L. 196 (2003).

rather than Australia.[251] The Australian High Court ruled that this case could be brought in Australia because that was the place of the "publication" that harmed his reputation, "Harm to reputation is done when a defamatory publication is comprehended by the reader, the listener, or the observer."[252]

A key aspect of Article 12's right to privacy, the right to be forgotten, has been taken up by a court with jurisdiction, converted into a fully enforceable online right, and turned over to a corporation for manifestation and enforcement. Other aspects, such as protection against online defamation, remain enforced case-by-case in regular courts as a component of tort law. ISP's in both instances seek to avoid liability but their efforts have produced mixed results. Other than GDPR in the EU, privacy as an Internet human rights appears to be a court-driven right rather than a legislative one. Therefore, continued monitoring of judicial activity in this area is necessary to chart further development.

Article 13: Freedom of Movement

Article 13 is divided into two freedoms of movement: within one's country, and across borders to and from other countries. The Internet is both border-bound, as to the ability of states to restrict digital movement within a country (that power typically stops at a state's borders), and borderless, as to both content and access—which in our globalized world are difficult to restrain to a specific state.[253] Article 13 states:

> (1) Everyone has the right to freedom of movement and residence within the borders of each state. (2) Everyone has the right to leave any country, including his own, and to return to his country.[254]

Applied to the Internet, this right ensures freedom of digital movement. So, for example under the first prong, one may move digitally *within* a country from one city to another unrestricted. Under the second prong, that same person should then be able to digitally move on from that country to another equally unimpeded. While it has been classically assumed that anyone can go anywhere on the Internet, "positive" regulation has been

---

[251] Reporters Committee for Freedom of the Press, *High Court Makes Landmark Ruling on Internet Jurisdiction in Libel Cases* (Dec. 10, 2002), https://www.rcfp.org/high-court-makes-landmark-ruling-internet-jurisdiction-libel-cases/ [https://perma.cc/D3WZ-SXRY].
[252] *Id.*
[253] *See* Toolkit, *supra* note 198 at 69–70.
[254] UDHR, *supra* note 17, at art. 13.

lacking. This has left space for countries to "negatively" regulate—effectively restricting freedom of digital movement as well as data portability, which allow individuals to move their own data from one service provider to another, enhancing the agency of people over their data[255].

Geoblocking restricts free digital movement across the global Internet based upon geographic location of the user that is determined via geolocation technology and by national laws.[256] With respect to a user being blocked based upon the country they logged onto the Internet from, the experience can be frustrating—for example not being able to stream a service that one has paid for or being not being able to use Wi-Fi enabled telecommunications from one country to the next.[257] How widespread is the geoblocking phenomenon? A 2018 study for the Internet Measurement Conference found that out of 177 countries studied, only one—Seychelles—did not have some form of geoblocking activity.[258]

However, geoblocking is a trend that is increasing.[259] Based upon geoblocking data shared for Cloudflare, AppEngine, and CloudFront, which host clients at the enterprise business level, according to one source, users in Russia, Iran, Cuba, Sudan, China, Nigeria, and Syria experienced the highest rates of being blocked based on their geographic location.[260]

It is possible to circumvent being geoblocked, but this evasion takes some effort and determination. Among the techniques used to access geoblocked content or services are remote access to computers in other countries, utilizing dial-up services to an ISP abroad, or resorting to file-sharing piracy techniques.[261] However, the most common form of circumvention is the use of a proxy. [262] Circumvention is a form of self-help to ensure one's unimpeded digital movement as an Internet human right, but it is not one that

---

[255] WORLD BANK GROUP, WORLD BANK DEVELOPMENT REPORT 2021: DATA FOR BETTER LIVES 204–205 (2021).
[256] Tal Kra-Oz, *Geoblocking and the Legality of Circumvention*, 57 IDEA- J. FRANKLIN PIERCE CENTER FOR INTELL. PROP. 385, 388 (2017).
[257] Maria José Schmidt-Kessen, *E.U. Digital Single Market Strategy, Digital Content and Geo-Blocking: Costs and Benefits of Partitioning E.U.'s Internal Market*, 24 COLUM. J. EUR. L. 561, 571 (2018).
[258] Allison McDonald et al., *403 Forbidden: A Global View of CDN Geoblocking*, PROCEEDINGS OF THE INTERNET MEASUREMENT CONFERENCE (2018) at 226.
[259] *Id.* at 229.
[260] *Id.* at 218.
[261] Kra-Oz, *supra* note 256, at 410.
[262] *Id.* at 411.

would be widely available to the general public given the level of technical knowledge and skill it requires.

With respect to those who are subjected to geoblocking, it cannot be assumed that every instance of blocking is actually blocking a *bona fide* human being entitled to Article 13's protection of free digital movement. Moreover, private corporations may engage in geoblocking for perfectly benign, market-driven reasons, or to comply with local government regulations.[263] Regardless of motive, however, the result remains the same—the potential for restriction of free digital movement by an individual, splintering of the internet, and potential removal of individuals from the digital market based on geographic location. It would not be hard to imagine a company targeting removal by postal code or telephone area code based upon that code's economic affluence or some other demographic feature. The reverse may be true as well. Companies may engage in predatory practices by targeting socio-economically poor geographic areas with predatory lending offers, thereby leaving out geographically affluent areas.

When considering its approach to this problem, the E.U. identified geoblocking as a significant threat to Europe's Single Market by perpetuating fragmentation in the digital realm.[264] That conclusion was borne out by data from consumer complaints: "74% of the complaints received by the European Consumer Centres Network regarding price differences or other geographical discrimination faced by consumers relate to online cross-border purchases."[265]

The European Union's response to excessive geoblocking activity came in the form of a regulation, adopted in 2018, to address the issue as it affects the Single Market.[266] The E.U.'s approach attempts to balance valid versus invalid geoblocking activity. Article 3 covers "Access to online transfers."[267] Similarly, Article 4 addresses access to goods or services.[268] This regulation is part of the E.U.'s Digital Single Market Strategy (DSMS), adopted in 2015 to identify and remove barriers to further single market integration in the

---

[263] McDonald, *supra* note 258, at 219.

[264] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe*, at 3 COM (2015) 192 final, (June 5, 2015).

[265] *Id.* at ¶ 2.3.

[266] *See generally* Commission Regulation 2018/302, 2018 O.J. (L 60I) (creating regulations addressing unjustified geoblocking).

[267] *Id.*, art. 3.

[268] *Id.*, art. 4.

digital sector which "could boost the EU economy by generating an additional 415 billion EUR in annual growth."[269]

Some argue, however, the E.U.'s DSMS is too ambitious, noting, "the European Union still is a patchwork of national online markets. This limits both the supply and demand of new digital services throughout Europe. According to the EC, 'persistent fragmentation is stifling Europe's competitiveness in the digital economy.'"[270] Together with widespread ambivalence towards Internet commerce in certain population sectors and fear of identity theft in others, the DSMS does not adequately take into account differences in digital development, for example, in the more advanced Scandinavian countries versus the less advanced southeast European states.[271] "Consequently, the DSMS is being developed against a backdrop of nascent rather than fully evolved digital engagement."[272]

Freedom of online movement is an area that remains unregulated. It is perhaps the oldest freedom assumed by the underlying structure of the Internet since its earliest days—namely that anyone can navigate anywhere to find anything. That underlying assumption of Internet operability, however, creates space for states, especially authoritarian states, to restrict freedom of online movement in furtherance of their own autocratic agendas. Consequently, until this freedom is guaranteed at the international level, or otherwise guarded by a large number of states, from a regulatory perspective, Article 13 will remain an assumption that can by undercut by states seeking to restrict movement.

Article 14: Right to Asylum

What is digital asylum? Article 14 of the UDHR provides:

> (1) Everyone has the right to seek and to enjoy in other countries asylum from persecution. (2) This right may not be invoked in the case of prosecutions genuinely arising from non-political crimes or

[269] Schmidt-Kessen, *supra* note 257, at 562.
[270] Stuart N. Brotman, *The European Union's Digital Single Market Strategy: A Conflict Between Government's Desire For Certainty And Rapid Marketplace Innovation?*, BROOKINGS 1, 2 (2016), https://www.brookings.edu/wp-content/uploads/2016/07/digital-single-market.pdf [https://perma.cc/CN8L-R9A8].

[271] *Id.*
[272] *Id.*

> from acts contrary to the purposes and principles of the United Nations.[273]

The closest analogues to this right may be freedoms from censorship and access to VPN's abroad, both discussed above. But with respect to asylum, context is important. The individual asserting this right must be persecuted for political reasons. Thus, a political activist in one country speaking out against their home government, whose social media platforms are hacked by the government or shut down completely, could feasibly assert an Article 14 right to access a social media platform in another country. If this individual attempted to avoid censorship via use of the Internet through an access point in another country, employment of a VPN would be the most likely method route to do so. [274]

VPN's are legal to use in many countries, but using one for illegal purposes is still illegal. Moreover, some states such as Russia, China, North Korea, and Iraq have banned their use entirely.[275] To capture the conduct of the political activist mentioned above, the law criminalizing use of VPN's in their home country would need to be drafted so as to encompass that individual's use of the VPN outside of the country as well as inside. Moreover, the intent aspect would need clarification—for example, some VPN's are used merely for privacy protection,[276] while others are used for entertainment. For example, some Netflix content is prohibited in certain contents; using a VPN allows users to circumvent internet blocks.[277] While this activity is arguably not illegal, it does violate Netflix's terms of use.[278]

But corporate permission is not so important as state permission. The entire premise of asylum law is that an individual is granted permission by a state to reside within that state once that person proves to the host state's satisfaction that they are being persecuted by their home state for political

---

[273] UDHR, *supra* note 17, at art. 14.
[274] *Understanding and Circumventing Network Censorship*, SURVEILLANCE SELF-DEFENSE, https://ssd.eff.org/en/module/understanding-and-circumventing-network-censorship [https://perma.cc/5JMG-HTDY] (last visited Apr. 19, 2023).
[275] Aaron Drapkin, *Are VPNs Legal? Your Rights to Using a VPN Explained*, TECH.CO (Mar. 31, 2023), https://tech.co/vpn/are-vpns-legal [https://perma.cc/U7L6-KUAL].
[276] J. Carlton Collins, *Protect Your Online Privacy with a VPN*, J. OF ACCOUNTANCY (June 1, 2018), https://www.journalofaccountancy.com/issues/2018/jun/vpn-for-businesses.html [https://perma.cc/623M-NLFM].
[277] Max Eddy, *How to Unblock Netflix with a VPN*, PC MAG. (Sept. 2, 2021), https://www.pcmag.com/how-to/how-to-unblock-netflix-with-a-vpn [https://perma.cc/59FT-DQRF].
[278] *Id.*

reasons.[279] Thus, for the digital version of Article 14 right to asylum to play out completely, our hypothetical political activist would need to access a state-sponsored (or contracted) VPN with in another country with permission once this dissident proves to that country that their home country is persecuting them. To date, no such VPN's have been made available by states to cyber-asylum seekers; however, that is not to say that it couldn't be done.

Perhaps the clearer analogy would be the Internet human right following the physical person into an asylum situation—such as Julian Assange being able to use the Internet within the Ecuadorian embassy in London where he was sheltered from British authorities for three years. Mr. Assange's digital asylum would be coterminous with his physical asylum.

Access to a VPN allows a person who is digitally persecuted or repressed to seek digital asylum and continue to enjoy the benefits of free political speech and thought. While a comprehensive body of asylum law has developed since the UDHR was promulgated, the likelihood of extending such rights into cyberspace is currently without much traction. For now, Article 14's promise of asylum in the online context is dependent upon an opportunistic marriage of an ingenuity and technological availability on an individual basis.

Article 15: Right to Nationality

"Digital citizenship" currently has no foundation beyond the physical location of where individuals are when accessing the Internet, an individual's Internet persona or in-line identity, and an individual's right to anonymity. The UDHR's Article 15 provides:

> (1) Everyone has the right to a nationality. (2) No one shall be arbitrarily deprived of his nationality nor denied the right to change his nationality.[280]

As mentioned above in the discussion relating to Article 6, digital identity is beyond the scope of this article. And while there are many ways in which a person can demonstrate or assert their on-line presence (through government issued identification numbers or credentials, biometric or

---

[279] *See* Deborah Anker, *The History and Future of Gender Asylum Law and Recognition of Domestic Violence as a Basis for Protection in the United States*, 45 HUM. RTS. 14, 14 (2020).

[280] UDHR, *supra* note 17, at art. 15.

biographic data, on-line authentication, or even electronic signatures), none of these, without additional evidence of legal status in a country, can be deemed to be proof of nationality.[281]

Nationality implies citizenship, and citizenship implies certain rights and responsibilities. However, the "space" of cyberspace is not limited to national frontiers. The citizenship, or nationality, of an individual on the Internet becomes important with respect to digitally effectuating this right when that individual is allowed or not allowed to do certain things on the Internet *because* of that citizenship or nationality.[282] For example, a German citizen's European citizenship allows them to take advantage of the EU-recognized right to be forgotten, and thereby request the restriction of search results about them in particular cases. However, even though the right to be forgotten is EU-wide, different countries in Europe take different approaches to personality torts, meaning an individual's national citizenship may still influence decisions.

By virtue of a person's legal status, an individual would be able to obtain a government-issued electronic identity. Government-issued electronic identities serve several purposes, including "identification, two-factor authentication to access online services (e.g., e-government services), electronic proof-of-passport information to allow access to personal data, and a legally effective electronic signature."[283] Some states are designing strategies for more comprehensive online identity management (IdM).[284] "For most countries, the overarching objective or vision for the development of a national IdM strategy is the realisation of electronic government" or provisions of government to citizen services.[285]

Estonia, for example, is considered a global leader in IdM.[286] Estonia's digital identity program allows for e-governance (99% of public services

---

[281] *Policy Brief: Identity on the Internet*, INTERNET SOC'Y (June 9, 2016), https://www.internetsociety.org/policybriefs/identity [https://perma.cc/99F6-3NBZ] [hereinafter *Policy Brief*].

[282] For purposes of this article, we equate "citizenship" with "nationality". Identity, especially "digital identity," is not necessarily linked with either citizenship or nationality.

[283] *Policy Brief*, *supra* note 281.

[284] *National Strategies and Policies for Digital Identity Management in OECD Countries*, *OECD Digital Economy Papers*, No. 177, OECD Report (Mar. 31, 2011).

[285] *Id.*

[286] Ott Vatter, *Why Estonia Pioneered Digital Identity*, TECH RADAR (Sept. 3, 2019), https://www.techradar.com/news/why-estonia-pioneered-digital-identity [https://perma.cc/G4QZ-6BV7]; Daniel Castro, *Explaining International Leadership: Electronic Identification Systems*, INF. TECH. & INNOVATION FOUND. REP., at 7 (Sept. 2011), https://itif.org/files/2011-e-id-report-final.pdf [https://perma.cc/2QJY-2MJS].

available online), filing of e-taxes, i-voting, cryptocurrency, e-residency, and e-health records.[287] Thus, by virtue of their Estonian citizenship, Estonian nationals receive a wide variety of electronic benefits.[288] This comprehensive program also arguably prevents capture of Estonian ex-pats by the other countries in which they are residing by keeping Estonians living abroad more completely connected to their state of citizenship, albeit remotely, in very tangible ways.[289]

Article 15, however, only guarantees the right to nationality, not to the extent of benefits which might derive therefrom—which will vary widely among countries, although it does enable individuals to change their citizenship. Thus, a national living in a low bandwidth country with low or poor access to on-line governmental purposes may seek to adopt a new nationality, but that may not necessarily change that person's access to higher capacity broadband or great on-line public services. At the same time. in this globalized world, nationals of one country frequently live in another, and are able to access governmental services via the Internet in both their home and host countries. So, it would appear that full enjoyment of this right on-line lies in its promise.

Digital citizenship is tethered to national citizenship and, therefore, comprehends some degree of state regulation. Although many states are beginning to develop online identity management schemes to access state benefits and services, it is still very much early days. Credentialing, attribution, and digital signatures, however, are all coming into their own. No one seriously doubts that the relationship between a state and its citizens in the physical world will gradually move to an online framework, if for no other reason than the increase in efficiencies and decrease in costs that an online framework offers both.

Article 16: Right to Marry and to Found a Family

Although perhaps not obvious, the right to create and grow a family unit is not one that is immune from online existence. Online dating, online

---

[287] *How Estonia is Pioneering the Digital Identity Space*, METADIUM (June 6, 2019), https://medium.com/metadium/how-estonia-is-pioneering-the-digital-identity-space-4008c709fbb8 [https://perma.cc/A2YV-CR6D].

[288] *Estonian e-ID Card: Entering the Contactless World*, INVEST IN ESTONIA (June 2017) https://investinestonia.com/estonian-eid-card-entering-the-contactless-world/ [https://perma.cc/26WY-UCYZ].

[289] Vatter, *supra* note 286.

weddings, online marriage, and the maintenance of online family life have grown dramatically during the COVID pandemic. The UDHR's Article 16 protects these rights:

> (1) Men and women of full age, without any limitation due to race, nationality or religion, have the right to marry and to found a family. They are entitled to equal rights as to marriage, during marriage and at its dissolution. (2) Marriage shall be entered into only with the free and full consent of the intending spouses. (3) The family is the natural and fundamental group unit of society and is entitled to protection by society and the State.[290]

This particular human right is perhaps more fraught with difficulty in implementation by divergent cultural and religious constraints of societies than any other right.[291] Those constraints may affect how the online platform works. For example, in more traditionally conservative societies, chaperones may be digitally involved in filtering those who can interact with dating-age family members, whereas in western societies, open-ended non-supervised interactions are the norm.[292] The western paradigm of individual autonomy in online dating may in fact be challenging the family's role in matchmaking common in more traditional societies.[293]

Nevertheless, it is a recognized right that is becoming more and more translatable to the digital world. Globally, 39% of online singles have used online dating sites or apps within the past month (measured in 2020).[294] In the United States, three in ten adults have used a dating site or app, but this number varies by age and sexual orientation.[295] Security concerns abound, as 46% of surveyed Americans believe dating sites and apps to be "not too safe"

---

[290] UDHR, *supra* note 17, at art. 16. These rights have been extended to same-sex couples in most Western industrialized states. *See Marriage Equality Around the World*, HUM. RTS. CAMPAIGN, https://www.hrc.org/resources/marriage-equality-around-the-world [https://perma.cc/98PN-DKBU].

[291] Annisa M.P. Rochadiat, Stephanie Tom Tong & Julie M. Novak, *Online Dating and Courtship Among Muslim American Women: Negotiating Technology, Religious Identity, and Culture*, 20 NEW MEDIA & SOCIETY 1, 5-8 (2017).

[292] *Id.*

[293] *Id.*; Jialin Li & Anna Lipscomb, *Love On the Cloud: The Rise of Online Dating in China*, US-CHINA TODAY, July 17, 2017.

[294] Tom Morris, *Dating in 2021: Swiping Left on COVID-19*, GWI. (Mar. 2, 2021), https://blog.globalwebindex.com/trends/online-dating/ [https://perma.cc/U2E3-AJHD].

[295] Emily A. Vogels, *10 Facts About Americans and Online Dating*, PEW RSCH. CTR. (Feb. 6, 2020), https://www.pewresearch.org/fact-tank/2020/02/06/10-facts-about-americans-and-online-dating/ [https://perma.cc/LZ9Y-LHA5].

or "not safe at all."[296] Yet, 54% of Americans say relationships that begin on dating sites and apps are just as successful as those that begin in person.[297] "Online dating is now so popular that studies suggest it is the third most common way to meet a partner in Germany and the US."[298]

In a nod to the "legal equivalence" of online contracts to those written on paper and signed with ink, even an on-line marriage can now be given legal recognition. Once partners find one another, the wedding that ensues takes all kinds of forms, but was already tentatively moving online prior to the COVID-19 pandemic as a cheaper alternative to the traditional wedding.[299] The pandemic significantly accelerated this process.[300] New York, responded very quickly to the new reality of legalizing marriages online during the pandemic. New York City's marriage bureau noted in 2020 that even though all components of getting married had moved online, the individuals involved in the ceremony process still had to be within New York's jurisdiction for the marriage to be legal.[301] California also moved quickly, empowering county clerks to "email your marriage license to you after a virtual conference as long as you meet the following requirements: both adults are located within the State of California, both adults are present during the video conference, and both adults can produce valid identification during the video conference."[302]

---

[296] *Id.*

[297] *Id.*

[298] Donna Ferguson, *How Online Dating Has Changed the Way We Fall in Love*, GUARDIAN (UK), Feb. 13, 2022.

[299] Daryl Nelson, *Getting Married Online is Becoming Big Business These Days*, CONSUMER AFF., (Apr. 4, 2013), https://www.consumeraffairs.com/news/getting-married-online-is-becoming-big-business-these-days-040413.html [https://perma.cc/2MSD-WL76].

[300] Olivia Harrison, *Is It Possible to Get Legally Married Online?*, REFINERY29 (May 29, 2020), https://www.refinery29.com/en-us/2020/05/9844333/can-you-get-married-online-coronavirus [https://perma.cc/2CLS-RTK8]; Haley Draznin, *Couples Around the World Are Livestreaming Their Weddings, Creating a Sense of 'Certainty' at an Uncertain Time*, CNN (Mar. 28, 2020), https://www.cnn.com/2020/03/28/us/couples-livestreaming-weddings-wellness-trnd/index.html [https://perma.cc/SE4T-6H4Y].

[301] *Marriage Frequently Asked Questions*, OFF. OF THE CITY CLERK FOR THE CITY OF N.Y., https://www.cityclerk.nyc.gov/content/marriage-frequently-asked-questions [https://perma.cc/M7MZ-SBD4] (last visited Apr. 19, 2023).

[302] E.A. Gjelten, *California Allows You to Get Married Online During the COVID-19 Pandemic*, DIVORCENET, https://www.divorcenet.com/resources/california-allows-you-to-get-married-online-during-covid-19-outbreak.html [https://perma.cc/6NJT-6V7G] (last visited Apr. 19, 2023).

Zoom and other platforms have allowed families to remain connected during the pandemic. However, digital divorce proceedings have not emerged the way digital marriage has. Uncontested divorce can largely be resolved online;[303] however, contested divorces are much more difficult to resolve via the Internet.[304] Like any other civil trial, some hearings and proceedings moved online during COVID, but are returning to live courtrooms as the pandemic draws to a close and COVID cases for an area fall.[305] Because the pandemic has driven much of the movement of rights associated with Article 16 online, it is unclear whether or how many governments will continue to maintain online platforms in this area after the pandemic recedes.

Like other aspects of life, key aspects of services leading to both marriage and divorce have migrated online. Yet family associated human rights remain so infused with local strictures and traditions, the cultural relativism trap is impossible to escape—even online. That said, as a human right, founding and managing a family remains such a key component to the individual fulfillment comprehended by the entire thrust of UDHR that Article 16's freedoms should be accorded more protection both at the state level and internationally.

Article 17: Right to Own Property

This article comprehends both ownership and deprivation. Article 17 of the UDHR states:

> (1) Everyone has the right to own property alone as well as in association with others. (2) No one shall be arbitrarily deprived of his property.[306]

Article 17 comprises both ownership and deprivation of property; it does not distinguish between real, tangible, intangible or intellectual property, but, as with all articles of the UDHR, its original application must be understood with reference to the kinds of property that were recognized at the time of its adoption. In the intervening decades, all sorts of property rights have been recognized in the context of cyberspace and on the Internet. While some of these property rights, including their means of enforcement, are beyond the

---

[303] Elizabeth Thornburg, *Observing Online Courts: Lessons from the Pandemic*, 54 FAM. L. Q. 181, 187 (2021).
[304] *Id.* at 223.
[305] *Id.* at 224.
[306] UDHR, *supra* note 17, at art. 17.

scope of this article (such as asserting rights in connection with the use of domain names[307] or corporate ownership of intellectual property[308] or "Big Data"), the principles of property ownership and enforcement of rights in those cases may be instructive, by analogy, for understanding the issues of

[307] Internet domain names provide an example, even though a full discussion of Internet governance is beyond the scope of this article. "An Internet domain name is a unique name of an organization or person on the Internet. The name is combined with a generic top-level domain (gTLD), such as .com or .org. . . . By 2019, there were more than 300 million registered domain names." *Internet Domain Name*, PC MAG. ENCYCLOPEDIA, https://www.pcmag.com/encyclopedia/term/internet-domain-name [https://perma.cc/DVS9-JVFU] (last visited June 18, 2021). Top-level domains (TLDs), consisting of a word or phrase at the far right had side of an email address, for example, are part to the domain name system (DNS) operated by ICANN (the Internet Corporation for Assigned Names and Numbers) enable finding websites and help direct Internet traffic. There are two types of TLDs: generic TLDs (or gTLDs, such as .org, .com, etc,) and country-code TLDs (or ccTLDs, such as .fr for France). Enforcement of rights in gTLDs is often associated with enforcement of trademark rights (*see, e.g.*, James Urzedwoski and Daniel A. Tysver, *Domain Name Disputes*, BITLAW GUIDANCE, https://www.bitlaw.com/internet/domain.html [https://perma.cc/XBZ8-K7X3] (last visited June 16, 2021). In the case of ccTLDs, countries do not "own" the ccTLDs associated with their countries. The two letter country codes used in ccTLDs can be found in Standard 3166 of the International Standards Organization (ISO). *See The International Standard for Country Codes and Codes for Their Subdivisions,* ISO 3166 COUNTY CODES, https://www.iso.org/iso-3166-country-codes.html [https://perma.cc/Z2B8-3XKH] (last visited Apr. 19, 2023). ccTLDs are assigned to countries or parties acting on behalf of countries through contract with ICANN, as such they create a right in contract, but not a property right. Domestically, victims can turn to the courts for relief. In the U.S., litigants traditionally rely upon trademark and dilution law; however, the 1999 Anti-Cybersquatting Consumer Protection Act "made it easier for individuals and companies to take over domain names that are confusingly similar to their names or valid trademarks. To do so, however, they must establish that the domain name holder acted in bad faith." ." Anti-Cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d) (1999). Relief can also be sought via the Uniform Domain Name Dispute Resolution Policy that "has been adopted by all ICANN-accredited registrars" to challenge appropriation of domain names. *See Uniform Domain-Name Dispute-Resolution Policy*, ICANN, https://www.icann.org/resources/pages/policy-2012-02-25-en [https://perma.cc/QY6M-4ERQ] (last visited Aug. 24, 2020).

[308] While intellectual property rights (IPRs) are not necessarily seen as human rights (especially where IPRs are owned by entities with legal personality), protecting artistic works, music, written works, patents, trademarks, ideas, etcetera which exist in cyberspace is not difficult to conceive. In addition to national law, the international basis of these rights can be found in the World Trade Organization's Trade-Related Aspects of Intellectual Property Rights (TRIPS). *Intellectual Property: Protection and Enforcement*, WORLD TRADE ORG., https://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm [https://perma.cc/F4R5-Y7JT] (last visited July 15, 2021).

how individuals might enforce their property rights in cyberspace and on the Internet under Article 17. At the same time, new forms of property and ownership have emerged in recent years (for example, nonfungible tokens (NFTs) and "rights" in VR, AR, and gaming), and the law around these rights is still evolving.

The Internet has made online theft easier and more difficult to trace.[309] "The absence of territorial limits on the Internet, along with the scope it offers for anonymity, has opened the door to infringements of intellectual property (IP) rights that are new in both nature and scale."[310] This is especially true in the entertainment industry.[311] The United States continues to lose "$58 billion annually due to online copyright piracy."[312] Big data itself can also be defined as property subject to protection.[313]

One of the newest forms of intellectual property, non-fungible tokens (NFTs) are unique in nature and occupy an evolving place in notions of cyberspace property.[314] NFTs are "one-of-a-kind" assets that have no tangible form of their own and exist on the blockchain.[315] Unlike bitcoins—which are identical and exchangeable and one still has a bitcoin when traded for another—NFTs only exist once and if one exchanges an NFT for another NFT, then one has a completely different NFT.[316] "NFTs can really be anything digital (such as drawings, music, your brain downloaded and turned

---

[309] Reggie Ash, *Protecting Intellectual Property and the Nation's Economic Security*, 6 LANDSLIDE 20 (2014).

[310] Heike Wollgast, *IP Infringements on the Internet – Some Legal Considerations*, WIPO MAG. (Jan. 2007), https://www.wipo.int/wipo_magazine/en/2007/01/article_0005.html [https://perma.cc/3K9J-PR87].

[311] Ash, *supra* note 309.

[312] *Id.* at 22.

[313] Valentina Manzo, The Internet of Things and Intellectual Property Rights: The Protection of Data (2018) (LL.M. thesis, University of Turin Law School) (SSRN).

[314] Brian Frye, *After Copyright, Pwning NFTs in a Clout Economy*, 45 COLUM. J. L. & ARTS 341, 345–47 (2022).

[315] *What Are NFTs and Why Are Some Worth Millions?*, BBC (Dec. 16, 2023), https://www.bbc.com/news/technology-56371912 [https://perma.cc/ERH2-645L]. While commonly thought of in connection with digital art, even a tweet can be a saleable NFT. Twitter's CEO, Jack Dorsey, sold his first tweet as an NFT for $2.9 million in 2021. Elizabeth Howcroft, *Twitter boss Jack Dorsey's first tweet sold for $2.9 million as an NFT,* REUTERS (Mar. 22, 2021, 1:50 PM) https://www.reuters.com/article/us-twitter-dorsey-nft-idUSKBN2BE2KJ [https://perma.cc/GG3J-RJQF].

[316] Mitchell Clark, *NFTs, Explained*, THE VERGE (June 6, 2022, 8:30 AM) https://www.theverge.com/22310188/nft-explainer-what-is-blockchain-crypto-art-faq [https://perma.cc/E592-9HDN].

into an AI), but a lot of the current excitement is around using the tech to sell digital art."[317]

A recent UK court case may shed light on, or at least reframe the discussion around, various aspects of the "property" nature of NFTs, including that the domicile of the claimant was the situs of the asset, and that the effective "control" over the asset creates a property right, confirming that the NFT should be thought of as a digital asset.[318] As such NFTs could thus be regulated like other (digital) assets.[319] Such regulation may go some way to ensuring consumer protection and thus shoring up the right to own property found in Article 17.

Finally, the "metaverse" poses questions about the application of Article 17 property rights. First among these is the question whether laws that were designed to protect rights of humans extend to avatars?[320] Next are definitional questions – what is the metaverse? Is it VR? AR? Gaming? Some combination of all three? Will avatars be able to own and dispose of property in the metaverse? However one defines the metaverse, property ownership in that metaverse will be stress-tested. Crucial uncertainties about the legal capacity of avatars to enter binding agreements in their own right must be resolved. Moreover, assuming an avatar's capacity can be imputed to a real person, what becomes of the "meeting of the minds" component of a binding contract when one of two avatars to the agreement is actually machine generated? AI will further exacerbate such uncertainties.

Likewise, there will be jurisdictional problems compounded by the physical location of the actual person, whether the VR is hosted in the cloud and where the cloud can be deemed to be, and if one avatar in one VR is interacting with another avatar in another VR, where is that avatar or VR deemed to be located?[321] Unlike certain metaverse predecessors, such as

---

[317] *Id.*

[318] *Property Rights in NFTs Are in the Spotlight*, JDSUPRA (Aug. 23, 2022), https://www.jdsupra.com/legalnews/property-rights-in-nfts-are-in-the-4248058/ [https://perma.cc/TF5U-YHT2].

[319] *Id.*

[320] Arguably, the data protection provisions of the European Union's General Data Protection Regulation (GDPR) may apply to avatars if one reads the definition of "personal data" in article 4(1) of the GDPR to mean that an avatar is data "relating to" an identifiable person. The text of article 4(1) reads in pertinent part, "'personal data' means any information *relating to*) emphasis added) an identified or identifiable natural person ('data subject')." Commission Regulation 2016/679. 2016 J.O. (L119) 1 (emphasis added).

[321] Jurisdictional problems about the location of property are not new to the Internet. In the famous *Yahoo France* series of cases a French court attempted to assert jurisdiction over the

Second Life,[322] which is a proprietary platform governed by terms of service, the metaverse is a polymorphic, evolving, multi-operator/service-provider environment in which a single terms of service that could govern the treatment of property rights and disputes does not necessarily exist. In the case of Second Life, one can "look under the hood" so to speak by examining its terms of service. In the metaverse context, because of multiple actors and the uncertainty about which rules apply, it is difficult to predict how a person could assert Article 17 property rights.

Finally, and though not directly related to Article 17, due to the cost and expense of VR and AR right now, as well as energy, data storage and bandwidth requirements, the metaverse may also be the source of the next "digital divide" potentially perpetuating inequalities and power asymmetries in terms of "access" between high-middle income and high-income countries on the one hand, and lower-middle and low-income countries on the other.

Article 18: Freedom of Thought, Religion, or Belief

Freedom of thought and religion are most vulnerable in authoritarian societies—be they totalitarian, theocratic, or otherwise despotic. During the 20th Century, communist societies were known for state policies of atheism, driving religious and intellectual groups underground—perhaps most famously in the Soviet Union,[323] but still play out in today's dictatorships, autocracies and theocracies.[324] Article 18 of the UDHR responds to such suppression by providing that:

---

sale of Nazi memorabilia on Yahoo.fr, claiming that under French law it was illegal to trade in such items. The matter was ultimately resolved by moving the sale to Yahoo.com. *See*, Marc Greenberg, *A Return to Lilliput: The LICRA v. Yahoo! Case and the Regulation of Online Content in the World Market*, 18, BERKELEY TECH. L.J. 1191, 1193 (2003). Likewise, the D'Aloia case may be instructive in the case of ownership of property in the metaverse – will arguments about indicia of control over digital "assets" be used to establish "property" rights of individuals in the metaverse? Fabrizio D'Aloia v. Persons Unknown & Others [2022] EWHC (Ch) 1723 (Eng.).

[322] *See Second Life Terms and Conditions*, SECOND LIFE, https://www.lindenlab.com/legal/second-life-terms-and-conditions, [https://perma.cc/ULN9-UQME].

[323] Paul Froese, *Forced Secularization in Soviet Russia: Why an Atheistic Monopoly Failed*, 43 J. SCI. STUDY OF RELIGION 35 (2004).

[324] U.S. DEP'T OF STATE, 2020 REPORT ON INTERNATIONAL RELIGIOUS FREEDOM: DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (DPRK) (2021); U.S. DEP'T OF STATE, 2020 REPORT ON INTERNATIONAL RELIGIOUS FREEDOM: CHINA (INCLUDES TIBET, XINJIANG, HONG KONG, AND MACAU) (2021); U.S. DEP'T OF STATE, 2020 REPORT ON INTERNATIONAL

> Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.[325]

The aspect of free thought protected by Article 18 is ideation. Once thoughts are expressed, other UDHR articles such as freedom of expression and privacy are triggered. So how does one keep a thought from forming? One way is thought control.

Article 18 also offers protection for freedom of religion and belief. In the context of cyberspace, this implicates state suppression or censorship. Free exercise need not be actual participation via a digital format in a specific religious rite, although it certainly can be. Free exercise can include expressions of faith,[326] which countries may try to repress. Online manifestations of traditional religions, for example: the website of a house of worship in country A, accessible via the Internet in country B, which digitally broadcasts daily services on the Internet may be targeted by the government in country B. That would be a straightforward case of suppression in violation of Article 18's protection of the Internet human right to religious freedom. Another example would be that same individual in country B logging onto a spiritual community that exists only online: a cyber-church.[327] Suppressing access would also violate Article 18.

A third example may involve the same individual in country B accessing multiple spiritual sources in a blended approach, such that this person is adapting various components of religions while realizing their own personalized spiritual journey.[328] When someone is essentially constructing their own online spiritual experience, highly tailored to their individual preferences, is suppression of this activity to be equated with suppression of religion? In other words, does the religion being suppressed need to be an

---

RELIGIOUS FREEDOM: SAUDI ARABIA (2021); and U.S. DEP'T OF STATE, 2020 REPORT ON INTERNATIONAL RELIGIOUS FREEDOM: IRAN (2021).

[325] UDHR, *supra* note 17, at art. 18.

[326] *Free Exercise of Religion*, ACLU, https://www.aclu.org/issues/religious-liberty/free-exercise-religion [https://perma.cc/RDG7-Q38Y] (last visited Mar. 29, 2023).

[327] Heidi Campbell, *Understanding the Relationship between Religion Online and Offline in a Networked Society*, 80 J. AM. ACADEMY OF RELIGION 64, 70–71 (2012).

[328] *Id.* at 79.

established religion? Article 18 is worded broadly to encompass beliefs—which would be protected in this example as well, thereby sidestepping the question of "what is a religion?" Migration of spirituality to the Internet has accelerated in the early 21st Century.[329] "As our culture has become wired, so has our faith."[330]

When suppression of religion or belief happens, it typically takes the form of censorship. Such censorship can be either substantive or pretextual. Censoring religious content, for example, can help enforce a theocratic regime's protection of the religious and moral norms of society, particularly in countries where religion plays a major role in the socio-political sphere.[331]

Other, non-theocratic countries, however, may take a more pretextual approach. Whether it is targeting sects,[332] or other religions with online presences, censorship is not so much for the sake of snuffing out religious content; rather, it is about attempting to control elements the state considers destabilizing to the order it imposed.[333] Laws targeting religious activity on the Internet often provide for a kind of registration that may include "moral fitness" requirements, which obviously run afoul of Article 18.

In response, some target groups establish external homes for their Internet activities to escape official surveillance. Uniquely, the Internet has in fact become an effective tool for the weak to fight back against state suppression—which is, of course, what authoritarian states fear most.

Freedom of thought, religion, and belief is closely aligned with freedom of expression—at least in the sense that formative ideas should have space to flourish. However, exercising such online rights in states ruled by authoritarian regimes for theocracies can be problematic at best. Thus, transference of Article 18's human rights to digital space will depend upon the enforceability of online strictures by such regimes. Free societies are less likely to encounter such online roadblocks.

Article 19: Freedom of Opinion and Expression

---

[329] Helland, *supra* note 326.
[330] *Id.*
[331] Alisa Shishkina & Leonid Isaev, *Internet Censorship in Arab Countries: Religious and Moral Aspects*, 9 RELIGIONS 358 (2018).
[332] June Cheng, *Suppressing Religion Online: A Draft Law Threatens the Future of Christian Websites in China*, WORLD MAG. (Oct. 18, 2018), https://wng.org/articles/suppressing-religion-online-1617300122 [https://perma.cc/C7P6-YG6W].
[333] *China to Regulate Online Suspicious Activity Amid Crackdown*, AP (Sept. 11, 2018), https://apnews.com/b08dc47d56a640a8b2d2540c8a81539f/China-to-regulate-online-religious-activity-amid-crackdown [https://perma.cc/Q2QX-8LGV].

There is a Janus-faced nature to free speech, simultaneously ensuring that one is able to make the speech while equally ensuring that another is able to receive the speech. Thus, Article 19 is crafted to provide:

> 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.[334]

States may characterize the central concept of this right in its digital form as a right to information that must be balanced against the protection of other rights as well as public interests. The Greek constitution, for example, was modified in the early 21st century to both incorporate this Internet human right while also striking that balance.[335] While not all states have lodged this protection in their constitutions with specific reference to Internet rights as Greece has, many have extended pre-existing legal protections ensuring freedom of expression to encompass protection of digital expression as well. Worldwide, freedom of information laws, constitutional amendments, or statutes for example have been passed in 119 countries.[336]

In 2011, the Special Rapporteur for the U.N.'s Human Rights Council asserted:

> By explicitly providing that everyone has the right to express him or herself through any media, the Special Rapporteur underscores that Article 19 of the Universal Declaration of Human Rights and the Covenant was drafted with foresight to include and to accommodate future technological developments through which individuals can exercise their right to freedom of expression.[337]

He went on to bridge this assertion specifically to cyberspace: "Hence, the framework of international human rights law remains relevant today and

---

[334] UDHR, *supra* note 17, at art. 19.
[335] 2019 Syntagma [Syn.] [Constitution] art. 5A (Greece).
[336] *Alphabetical and Chronological Lists of Countries with FOI Regimes*, FREEDOMINFO (Sep. 28, 2017), https://www.freedominfo.org/2017/09/chronological-and-alphabetical-lists-of-countries-with-foi-regimes/ [https://perma.cc/HM4V-3JLW].
[337] Frank LaRue (Special Rapporteur), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, U.N. Doc. A/HRC/17/27 (May 16, 2011).

equally applicable to new communication technologies such as the Internet."[338]

A second Special Rapporteur buttressed this central assertion, [339] and the U.N. Human Rights Council followed these reports with adoption of Resolution 32/13, which "condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law, and calls upon all States to refrain from and cease such measures."[340] Regionally, the European Union and the African Commission on Human and People's Rights are in accord.[341] Internationally, there is consistent admonition supporting Article 19's global migration to cyberspace as an Internet human right instead of the regional movement to digital space now in progress.

Liberia became the first West African country to pass a law guaranteeing protection to information access by passing the Freedom of Information Law in 2010.[342] Liberia's Freedom of Information Act[343] allows individuals the right to "information held by public bodies and private entities that receive public funds or perform public functions."[344] Access to this information is not conditioned on providing a reason for wanting to see this information.[345] The U.N. has also taken steps to ensuring "public access to information . . . in accordance with national legislation and international agreements."[346]

Nevertheless, qualifiers such as those in the Greek constitution are often embedded with the digital free expression language. These can give rise to pretexts for censorship. Moreover, freedom of expression has a greater proclivity to collide with other rights than do most other freedoms; therefore, a state's balancing approaches can serve as yet another basis for digital

---

[338] *Id.*

[339] David Kaye (Special Rapporteur), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, GA, HRC, Report at ¶ 65–72, Doc. A/HRC/38/35 (April 6, 2018).

[340] Hum. Rts. Council Res. 32/13, U.N. Doc. A/HRC/RES/32/13 (July 18, 2016).

[341] Afr. Comm'n on Hum. and Peoples' Rts. Res. 362, ACHPR/Res.362(LIX)2016 (Nov. 4, 2016)

[342] THE CARTER CTR., CITIZEN'S GUIDE TO THE 2010 LIBERIA FOI ACT 3 (last accessed Oct. 15, 2021), available at https://www.cartercenter.org/resources/pdfs/peace/ati/liberia/citizens-guide-to-foi-final.pdf.

[343]Freedom of Information Act (2010) (Liber.)..

[344] THE CARTER CTR., *supra* note **Error! Bookmark not defined.**, at 10.

[345] *Id.*

[346] U.N. EDUC., SCI., AND CULTURAL ORG., TO RECOVERY AND BEYOND: 2021 UNESCO REPORT ON PUBLIC ACCESS TO INFORMATION 6 (2022).

restriction. The International Covenant on Civil and Political Rights offers a framework for states to follow when such restrictions are necessary. [347]

No region is immune from attempts at censorship, and while it is governments in some regions doing the censoring, it is the private sector in others.[348] Additionally, governments deploy a variety of means to restrict (or make it difficult to) access to content including criminalizing certain activity, blocking social media sites (for example, during anti-government protests),[349] issuing taxes on social media,[350] and erecting technological barriers to access content.[351]

But many governments do not have the luxury of blocking websites or throttling bandwidth. New Zealand's response to the Spring 2019 terrorist attack in Christchurch is one example.[352] "In the aftermath of the New Zealand attack, several major Internet Service Providers across New Zealand blocked access nation-wide to an opaque list of websites believed to be either hosting copies of the attack video or sensitive details of the attack."[353] However, pushback in open societies with freedom of speech as a core liberty challenges the notion that people should be spared the distress of watching such atrocities unfold.[354]

---

[347] Amy E. Cattle, comment, *Digital Tahrir Square: An Analysis of Human Rights and the Internet Examined through the Lens of the Egyptian Arab Spring*, 26 DUKE J. COMP. & INT'L L. 417, 423 (2016).

[348] *See, e.g.*, Adrian Shahbaz, *The Rise of Digital Authoritarianism*, FREEDOM HOUSE (2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism [https://perma.cc/H2UY-PHCB].

[349] *See* Christopher Giles & Peter Mwai, *Africa Internet: Where and how are governments blocking it?*, BBC (Jan. 14, 2021), https://www.bbc.com/news/world-africa-47734843 [https://perma.cc/XLZ5-7THA] (discussing government restrictions on internet and social media access).

[350] Jenny Gathright, *Kenya's Crackdown on Fake News Raises Questions About Press Freedom*, NPR (May 19, 2018), https://www.npr.org/sections/thetwo-way/2018/05/19/612649393/kenyas-crackdown-on-fake-news-raises-questions-about-press-freedom [https://perma.cc/P8HK-Y9UP] (discussing a law in Kenya that allows for fines up to $50,000 for publishing false information).

[351] CONG.-EXEC. COMM'N ON CHINA, BLOCKING, FILTERING AND MONITORING (last visited July 30, 2021), https://www.cecc.gov/blocking-filtering-and-monitoring [https://perma.cc/YVB8-CFFN] (discussing China's internet censorship).

[352] *Christchurch Shootings: 49 Dead in New Zealand Mosque Attacks*, BBC (March 15, 2019), https://www.bbc.com/news/world-asia-47578798 [https://perma.cc/LDS2-9FYW].

[353] Kalev Leetaru, *Internet Blacklisting Is Taking Off Across the World*, FORBES (Mar. 21, 2019), https://www.forbes.com/sites/kalevleetaru/2019/03/21/internet-blacklisting-is-taking-off-across-the-world/?sh=b6f46e950cc2 [https://perma.cc/7GBS-UT9P].

[354] *Id.*

In the United States, the government is restricted from making such requests to Big Tech. First Amendment rights to freedom of expression have been extended to the Internet. In 2020, the Fourth Circuit Court of Appeals upheld a lower court's ruling that a local government official's Facebook page was a public forum under the First Amendment.[355]

> This is the first ruling from a federal appeals court to call a Facebook page a public forum, making it illegal for government officials to discriminate on the basis of viewpoint in administering the page.[356]

Likewise, in *Knight First Amendment Institute at Columbia University v. Trump*,[357] the Second Circuit Court of Appeals held that President Trump's Twitter accounts, @realdonaldtrump and @POTUS were both violating the First Amendment by blocking individuals from viewing those accounts.[358] However, as discussed in the next section with respect to freedom of assembly, law enforcement does possess "kill switch" capabilities with respect to cellular service that theoretically could be utilized during assembly events that turn dangerous.

When censorship does happen, such as banning Donald Trump from Twitter, Facebook, and YouTube in the wake of the January 6, 2021 insurrection, it is on the initiative of Big Tech, not at the request of the government.[359] Twitter's corporate journey since that decision has been calamitous (and very expensive) to say the least. It was later bought by the world's richest man, Elon Musk, who sought to have Trump returned to the platform.[360] His chaotic takeover devalued the company while he also fired

---

[355] Davison v. Randall, 912 F.3d 666 (4th Cir. 2019).
[356] Stephen Carr, *Local Official's Facebook Page Found to Be a Public Forum*, 46 LITIG. NEWS 22, 22 (2021).
[357] 928 F.3d 226 (2d. Cir. 2019).
[358] Caroline Harting, *Trump's Twitter Channel Is a Public Forum*, COLUM. NEWS (July 9, 2019), https://news.columbia.edu/news/trump-twitter-first-amendment [https://perma.cc/DYJ5-W4XJ].
[359] Hannah Denham, *These Are the Platforms That Have Banned Trump and His Allies*, WASH. POST (Jan. 14, 2021), https://www.washingtonpost.com/technology/2021/01/11/trump-banned-social-media/ [https://perma.cc/FEK7-T24B].
[360] Sheera Frenkel & Kate Conger, *Hate Speech's Rise on Twitter is Unprecedented, Researchers Find*, N.Y. TIMES (Dec. 2, 2022), https://www.nytimes.com/2022/12/02/technology/twitter-hate-speech.html [https://perma.cc/L9FY-AQGE].

half the workforce.[361] Musk's mantra of bringing free speech back to the platform[362] was immediately undermined by banning critiques of him on Twitter.[363]

Because he took this public company private, he will be able to call the shots. As Professor Etic Talley of Columbia Law School notes, "I expect Mr. Musk will run it as a somewhat friendly dictatorship."[364] Recognizing this new reality of a single person possessing vast power over digital free speech rights, the U.N. High Commissioner issued an open letter shortly after the takeover of Twitter reminding Musk "of the platform's responsibility 'to avoid amplifying content that results in harms to people's rights."[365] That admonition, however, had no effect on the spike in hate speech appearing on Twitter in the wake of Mr. Musk's takeover:

> Before Elon Musk bought Twitter, slurs against Black Americans showed up on the social media service an average of 1,282 times a day. After the billionaire became Twitter's owner, they jumped to 3,876 times a day.
>
> Slurs against gay men appeared on Twitter 2,506 times a day on average before Mr. Musk took over. Afterward, their use rose to 3,964 times a day.
>
> And antisemitic posts referring to Jews or Judaism soared more than 61 percent in the two weeks after Mr. Musk acquired the site.[366]

---

[361] Nicole Hasler, *A Bird in the Hand is Worth $44 Billion: Elon Musk's Twitter Takeover and What it Means*, OXFORD STUDENT (Nov. 17, 2022), https://www.oxfordstudent.com/2022/11/17/a-bird-in-the-hand-is-worth-44-billion-elon-musks-twitter-takeover-and-what-it-means/ [https://perma.cc/K8YQ-GQEY].

[362] Dana Hull et al., *Sarah, Frier, Maxwell Adler & Bloomberg, Elon Musk Says He Wants Twitter to Be a Free-Speech Bastion but His Companies Have a Long History of Silencing Critics*, FORTUNE (Apr. 22, 2022), https://fortune.com/2022/04/22/elon-musk-twitter-free-speech-tesla-spacex-long-history-silencing-critics/ [https://perma.cc/MHD3-M6ST].

[363] Billy Perrigo, *Twitter Bans Accounts Mocking 'Free Speech Absolutist' Elon Musk*, TIME (Nov. 7, 2022), https://time.com/6229960/twitter-bans-accounts-elon-musk-impersonators/ [https://perma.cc/VEE6-T4BG].

[364] Conger, *supra* note 36.

[365] Nick Cumming-Bruce, *Meet the World's New Human Rights Crisis Manager. He Has a Lot to Do.*, N.Y. TIMES (updated Nov. 24, 2022), https://www.nytimes.com/2022/11/24/world/europe/volker-turk-un-human-rights.html [https://perma.cc/W93Z-J5X4].

[366] Frenkel & Conger, supra note 360.

Even if the government is not engaged in what may be perceived as suppression of free speech, legal action can potentially serve as a remedy as well. Frustrated at the initiatives of Big Tech in the United States banning the false information narratives some politicians are attempting to challenge legislation that shields social media from liability.[367] Currently, censorship by social media outlets in the United States is difficult to contest.[368]

Perhaps no other UDHR right is as endemic to Internet use than freedom of expression. The digital give and take of information, ideas, and creative work is among the chief benefits that online life has to offer. As a classic speech right, Article 19 as a digital right belongs to both online speakers and listeners. Information flow in this manner is accelerated and facilitated by social media platforms, which can regulate that flow up to the point of censorship. Once that line is crossed, however, either by tech companies or governments, freedom of expression is imperiled. Thus, guidelines in the absence of regulation would be most welcome—especially for institutions engaged in balancing, for example, privacy rights against free expression rights.

Article 20: Freedom of Assembly and Association

Digital assembly and association can take a wide variety of forms. Access to social media groups, chatrooms, and blogs are the most common settings for this right to be implicated.[369] However, the prevalence of Zoom videoconferencing during the COVID-19 pandemic and its widespread adoption as the platform of preference to hold remote meetings, is a new and significant entry into this group.[370] The UDHR's Article 20 provides:

---

[367] Danielle Keats Citron & Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform*, 2020 UNIV. CHICAGO LEGAL FORUM 45 (2020).

[368] VALERIE C. BRANNON, CONG. RESEARCH SERV., R 45650, FREE SPEECH AND THE REGULATION OF SOCIAL MEDIA CONTENT, 1 (2019).

[369] *See, e.g.*, *Is Chat-Room Speech Protected?*, WIRED (Mar. 5, 2003), https://www.wired.com/2003/03/is-chat-room-speech-protected/ [https://perma.cc/X9CT-XQDZ] (likening internet chat rooms to anonymous pamphleteering); *Message Boards and Chat Rooms: Can They Be Regulated?*, FINDLAW (Mar. 26, 2008), https://corporate.findlaw.com/law-library/message-boards-and-chat-rooms-can-they-be-regulated.html [https://perma.cc/X9PJ-6XPC] (likening internet chat rooms to public fora).

[370] Roger Dooley, *How Zoom Conquered Video Conferencing*, FORBES (Sept. 30, 2020), https://www.forbes.com/sites/rogerdooley/2020/09/30/how-zoom-conquered-video-conferencing/?sh=75d6b3815a97 [https://perma.cc/QU95-AAYQ].

> (1) Everyone has the right to freedom of peaceful assembly and association. (2) No one may be compelled to belong to an association.[371]

The U.N. regards this right as extendable to the Internet. "The rights to freedom of peaceful assembly and of association are protected in Article 20 of the Universal Declaration of Human Rights . . . . The Human Rights Council has emphasized that States have the obligation to respect and fully protect these rights online as well as offline."[372] The second part of Article 20 has not yet manifested in digital space; so far nobody has been compelled to join an online group. The first part, however, is where government suppression of free assembly/association comes into play.

The bright line between when states should and should not suppress assembly is typically the line between peace and violence—a line that is sometimes crossed in the context of political protest. How a government characterizes protests as violence is key; such characterizations are as varied in nature as the governments that make them, although authoritarian regimes are more likely to use pretexts to shut down assemblies protesting against their rule.[373] Objectivity in threat assessments is hard to come by.

The digital version of Article 20's protection was perhaps best described by former U.S. Secretary of State Hilary Clinton: "The freedom to connect is like the freedom of assembly, only in cyberspace."[374] Social connections create online groups. Online groups can exist for literally minutes (as three people work together on a shared Google document or in a Zoom breakout room), or for much longer periods.[375]

Social media platforms, live-streaming tools, and communication apps played a key role in the "velvet" revolution of 2018 that led to the resignation

---

[371] UDHR, *supra* note 17, at art. 20.

[372] Clément Nyaletsossi Voule (Special Rapporteur), *Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and Association*, ¶ 10, U.N. Doc. A/HRC/41/41 (May 17, 2019)..

[373] *See, e.g.*, Paul Mozur, *In Hong Kong, A Proxy Battle Over Internet Freedom Begins*, N.Y. TIMES (updated Oct. 11, 2021), https://www.nytimes.com/2020/07/07/business/hong-kong-security-law-tech.html [https://perma.cc/ZQ2X-EZCJ]; Jeremy Hsu, *Fear of Internet Censorship Hangs Over Hong Kong Protests*, IEEE SPECTRUM (Nov. 22, 2019), https://spectrum.ieee.org/fear-of-internet-censorship-hangs-over-hong-kong-protests [https://perma.cc/Y6A5-B3TW].

[374] Douglas Rutzen & Jacob Zenn, *Association and Assembly in the Digital Age*, 13 INT'L J. NOT-FOR-PROFIT L. 54, 66 (Dec. 2011).

[375] *Is Chat-Room Speech Protected*?, *supra* note **Error! Bookmark not defined.**.

of the Prime Minister of Armenia.[376] Social media has played a critical role in the #BLM movement in the United States, the #RoadSafetyMovement in Bangladesh, the #FeesMustFall campaign in South Africa, and the global #ClimateStrikes and #MeToo movements.[377] "Through the use of social media, e-petitions and crowdfunding platforms, civil society organizations have been able to reach new audiences, spread information, attract members and find funding in ways that were previously impossible or extremely costly."[378]

It is precisely the increased threat of change such Internet-based movements pose that triggers government repression. Actions states take to assert control include imposing legal restrictions, criminalizing certain online activities, arbitrarily blocking online content, government-sponsored trolling and cyberattacks, network disruptions, social media tax, and surveillance.[379] With respect to trolling, the government instructs Internet trolls to disseminate propaganda online to disrupt/inhibit anti-government movements.[380]

Police use of "kill switches" to shut down cell phones of crowds gathering around crimes scenes, arrests, or other law enforcement activity taking place in public is certainly an impediment to free association.[381] Assembly needn't be planned in advance; it can occur spontaneously—perhaps provoked by the police activity itself. The spontaneous assembly of citizens around the Minneapolis metropolitan police officers who were in the process of slowly murdering George Floyd in May, 2020,[382] would likely have been an assembly in physical space protected by Article 20. An extension of that assembly in digital space included the many texts, photos, videos, electronic conversations, tweets, and other documentation of the crime. If police had used a kill switch to shut down the digital aspect of this spontaneous assembly, Article 20 would have been violated as an Internet human right

---

[376] Voule, *supra* note 348, at 6.
[377] *Id.*
[378] *Id.* at 7.
[379] *Id.* at 10–13.
[380] *Id.*
[381] Kit O'Connell, *Secretive Internet 'Kill Switch' and Apple Patent Could Stop You from Filming Police & Protests*, MINT PRESS NEWS (July 13, 2016), https://www.mintpressnews.com/secretive-internet-kill-switch-apple-patent-stop-activists-filming-police-protests/218383/ [https://perma.cc/3KHE-9UAU].
[382] Evan Hill et al., *How George Floyd Was Killed While in Police Custody*, N.Y. TIMES (Jan. 24, 2022), https://www.nytimes.com/2020/05/31/us/george-floyd-investigation.html [https://perma.cc/BT6Q-F4RU].

even if the people were not physically dispersed in the real world. Courts have not yet stopped development of such devices in the United States.[383]

Article 20's protection of online association and assembly as an Internet human right embraces both regularized assembly, such as for a weekly quilting group chatting as they stitch, and spontaneous temporary assembly, such as quickly formed WhatsApp groups chatting their way through the streets of Austin, Texas as part of the larger Black Lives Matter protest. The purpose of the assembly should not be determinative of the exercise of the right; however, it is the purpose that provides the pretext for autocratic regimes to crackdown on political protests and for police units even in western democracies to keep people at bay during controversial police actions. More advancement at the state level and internationally is needed in this regard.

Article 21: Democratic Participation

Democracy's movement to an online platform is best characterized as gradual, if not tentative. "A short course in democracy" is how many refer to UDHR's Article 21, including the U.N.'s Office of the High Commissioner for Human Rights.[384] Although the term democracy is not expressly used in the text,[385] the key principles undergirding the machinery of democracy are clearly outlined:

> (1) Everyone has the right to take part in the government of his country, directly or through freely chosen representatives. (2) Everyone has the right of equal access to public service in his country. (3) The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.[386]

---

[383] David Kravets, *Supreme Court Won't Force DHS to Reveal Secret Plan to Cut Cell Service*, ARS TECHNICA (Jan. 12, 2016), https://arstechnica.com/tech-policy/2016/01/supreme-court-wont-force-dhs-to-reveal-secret-plan-to-cut-cell-service/ [https://perma.cc/9GFK-N4TH].

[384] U.N. High Commissioner for Human Rights, *Universal Declaration of Human Rights at 70: 30 Articles on 30 Articles – Article 21*, OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS (Nov. 30 2018).

[385] UDHR, *supra* note 17, at art. 21.

[386] *Id.*

Guaranteeing the apparatus of democracies as fundamental human rights in and of themselves is foundational for achieving all the other human rights. The first two aspects of Article 21, participation in government and equal access to public service, take the form of sustained and meaningful discourse via cyberspace. Communication with elected representatives is more or less interactive depending on the mode of communication and societal norms. "Social media has become a key element of political discourse in many countries, allowing legislators to express their opinions, share information and connect with constituents online."[387]

Among legislators who tweet, those in the United States and U.K. do so most frequently.[388] Likewise, necessary communication to become an elected representative may depend upon filters put in place by various political parties that control slates of candidates. But the traditional political party control mechanisms are at least eroding in the Internet age if not transforming altogether.[389]

Political participation in the form of civic engagement can manifest in a variety of digital ways, including tracking legislation online, viewing legislative floor debates and committee hearings via the Internet[390] and live blogging, virtually attending judicial proceedings, or engaging in public advocacy through online petitions. Of these, electronic petitions have digitally united the public and governments more interactively than the other forms of engagement. Governments are increasingly accepting e-petitions in Australia, Canada, Germany, South Korea, Italy, Lithuania, Ireland, Portugal, Luxembourg, Austria, the United States, the Netherlands, and the U.K.[391] Of these, the German Bundestag has perhaps developed the most inclusive and responsive e-petition system, launched in 2008, by designating a parliamentary committee as an intake and evaluation filter with significant

---

[387] Kat Devlin et al., *For Global Legislators on Twitter, an Engaged Minority Creates Outsize Share of Content*, PEW RES. CTR. (May 18, 2020), https://www.pewresearch.org/global/2020/05/18/for-global-legislators-on-twitter-an-engaged-minority-creates-outsize-share-of-content/ [https://perma.cc/SK6F-Z2NG].

[388] *Id.*

[389] JAMIE BARTLETT & HEATHER GRABBE, E-DEMOCRACY IN THE EU: THE OPPORTUNITIES FOR DIGITAL POLITICS TO RE-ENGAGE VOTERS AND THE RISKS OF DISAPPOINTMENT 4 (Dec. 2015).

[390] *See generally Legislative Broadcasts and Webcasts*, NAT'L CONF. OF STATE LEGIS. (May 27, 2022), https://www.ncsl.org/research/about-state-legislatures/legislative-webcasts-and-broadcasts.aspx [https://perma.cc/LF6U-B6UH] (containing live broadcasts of legislative hearings)

[391] Caitlin Grover, *E-Petitions*, VICT. PARL. LIB. & INFO. SERV. 6 (2016) (Austl.), https://www.parliament.vic.gov.au/publications/research-papers/download/36-research-papers/13765-e-petition-research-paper-august2016 [https://perma.cc/JS3L-G6UP].

reporting requirements that also has the power to initiate investigations and hold hearings in response to verified petitions that pass a designated threshold of signatures.[392]

Shortly after the legislative branch was opened up to e-petitions in Germany, the executive branch in the United States launched an e-petition platform as part of the Obama administration's Open Government Initiative known as "We the People."[393] Although the President's "goal was to make the federal government more transparent, participatory and collaborative through the use of new technologies," the impacts of e-petitions were varied. That said, a 2013 e-petition requesting it be made "illegal for telephone companies to 'lock' their phones by preventing a phone purchased from one telephone carrier to be used on another carrier's system" led directly to legislation tackling this issue in 2014.[394] The White House initially set the limit of signatures at 5,000 for e-petitions to appear on the system, but soon raised that trigger to 10,000.[395]

Internet voting implicates the third prong of Article 21. The "universal and equal suffrage" election requirements clearly concern connectivity and perhaps net neutrality in digital space.[396] However, such connection may only be triggered when societies fully migrate to Internet-based voting platforms which, to date, has not yet happened. Internet voting is distinct from, and much less prevalent than, electronic voting.[397]

Bringing the voting interface to individual smart phones as true Internet voting is the mission of a new joint venture between a Danish tech firm and an American election research nonprofit led by Uber's former political advisor, who told NPR, "My goal is to make it possible for every single person in this country to vote in every single election on their phone."[398]

---

[392] *Id.* at 14–16; Thomas Saalfeld & Ralf Dobmeier, *The Bundestag and German Citizens: More Communication, Growing Distance*, 18 J. LEGIS. STUD. 314, 315 (2012).
[393] Paul Hitlin, *'We the People': Five Years of Online Petitions*, PEW RES. CTR. at 2 (Dec. 28, 2016), https://www.pewresearch.org/internet/2016/12/28/we-the-people-five-years-of-online-petitions/ [https://perma.cc/5PNB-9FPN].
[394] *Id.* at 3.
[395] *Id.* at 5.
[396] UDHR, *supra* note 17, at art. 21(3).
[397] *Countries that Use Internet Voting*, EUR. PARL. RSCH. SERV. (Sept. 12, 2018) https://epthinktank.eu/2018/09/12/digital-technology-in-elections-efficiency-versus-credibility/internet_voting_countries/ [https://perma.cc/K4V4-6X29].
[398] Miles Parks, *The Push for Internet Voting Continues, Mostly Thanks to One Guy*, NPR, (Sept. 30, 2021), https://www.npr.org/2021/09/30/1040999446/internet-voting-phones-tusk-grant [https://perma.cc/G894-HYJC].

Although an array of security concerns fuel broad dismissiveness about such a vision,[399] the technology of which has not been utilized beyond allowing overseas military personnel or persons with disabilities to vote,[400] the new consortium argues that end-to-end verification should overcome most of those concerns.[401]

Estonia is the leader in this field, allowing online elections since 2005.[402] In 2019, 43.7% of Estonian voted on the Internet—a significant jump from the 2% who voted online in 2005,[403] perhaps indicating that voters need a bit of time to become comfortable with the process or acclimated to it. Along with Canada, Australia, and France, the United States has also recently experimented with Internet voting.[404] "Thirty-two states and the District of Columbia offer some sort of internet voting through fax, e-mail or an online portal. In many cases, state departments collaborate with private election technology companies to run online elections."[405] However, security concerns bedeviled elections in West Virginia and Delaware, and Internet voting access remains largely limited to people in special circumstances who are, in most cases, willing to give up their anonymity.[406]

Until such time as Internet voting becomes widely adopted, the cyber aspect of Article 21's voting language centers on electronic voting, which can refer to an array of technologies related to vote counting, scanning, certifying,

---

[399] *See, e.g.*, Lily Hay Newman, *Voting Machines Are Still Absurdly Vulnerable to Attacks*, WIRED (Sept. 28, 2018), https://www.wired.com/story/voting-machine-vulnerabilities-defcon-voting-village/ [https://perma.cc/X48R-LGGC]; Ben Gilbert, *The Iowa Democratic Caucuses Were Plagued by Tech Problems That Reportedly Went Far Beyond Issues with an App*, BUS. INSIDER (Feb. 10, 2020), https://www.businessinsider.com/iowa-democratic-caucus-tech-issues-2020-2 [https://perma.cc/4WUX-2MBJ].

[400] Matt Vasilogambros & Lindsey Van Ness, *Despite Security Concerns, Online Voting Advances*, PEW TRUSTS (Feb. 17, 2021), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/02/17/despite-security-concerns-online-voting-advances [https://perma.cc/YL2D-JAJT].

[401] Parks, *supra* note 398.

[402] Eric Geller, *Some States Have Embraced Online Voting. It's a Huge Risk.*, POLITICO (June 9, 2020), https://www.politico.com/news/2020/06/08/online-voting-304013 [https://perma.cc/F55M-FPGU].

[403] *When Will Other Countries Join Estonia In Voting On The Internet?*, E-ESTONIA (Aug. 28, 2019), https://e-estonia.com/when-will-other-countries-join-estonia-in-voting-on-the-internet/ [https://perma.cc/YQ7M-W7UZ].

[404] Juhohn Lee, *Here's Why Most Americans Are Not Able to Vote Online in 2020*, CNBC (Sept. 23 2020), https://www.cnbc.com/2020/09/23/why-us-cant-vote-online-in-2020-presidential-election-trump-biden.html [https://perma.cc/9VCC-NU2W].

[405] *Id.*

[406] *Id.*

machine-to-machine communication, optical scanning voter identification,[407] or even facial recognition—a technology which could solve verification concerns but simultaneously trigger countervailing privacy issues.[408] Approximately 30 countries have adopted partial electronic voting systems for municipal, provincial/state, and national elections in some aspect of their election process with varying degrees of success.

Article 22: Right to Social Security & Self-Realization

Self-realization is a concept not unknown to political actors. Indeed, Thomas Jefferson inserted an inalienable right to the "pursuit of happiness" in the American Declaration of Independence, drawing upon the ancient Greek conception of, essentially, self-realization as the ideal end resulting in happiness.[409] Creating space for individuals to develop to their full potential necessitates more emphasis on personal freedom and restraint of government. Article 22 places this notion in modern language:

> Everyone, as a member of society, has the right to social security and is entitled to realization, through national effort and international co-operation and in accordance with the organization and resources of each State, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality.[410]

The first twenty years of Internet history went largely unregulated, allowing maximum space for personal development. From an Internet human rights perspective, the term "economic, social, and cultural rights" (ESCRs) are those comprehended here collectively (work, rest, education, culture, housing, health, etcetera), although they are each articulated individually and with more specificity in Articles 23-27. They are necessary for full self-realization in both non-digital and digital space, yet their development in digital space has been lagging.

---

[407] Rob Lundie, *Electronic Voting at Federal Elections*, PARLIAMENT OF AUSTRALIA (2016), https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook45p/ElectronicVoting [https://perma.cc/HE8J-5H9S].

[408] *See* Sven Heilberg et al., *Facial Recognition for Remote Electronic Voting – Missing Piece of the Puzzle or Yet Another Liability?*, *in* EMERGING TECH. FOR AUTHORIZATION & AUTHENTICATION 77 (Andrea Saracino & Paolo Mori eds., 2021).

[409] Herbert Lawrence Ganter, *Jefferson's "Pursuit of Happiness" and Some Forgotten Men*, 16 WM. & MARY Q. 558, 558–59 n.29 (1936).

[410] UDHR, *supra* note 17, at art. 22.

> At both the global and national levels, internet policy and regulation are not focused on creating an enabling environment for advancing ESCRs. Where policies do address links between internet regulation and human rights, they have done so almost exclusively in relation to civil and political rights—and most of these efforts have been driven by developed countries.[411]

Even so, manifestation of digital self-realization may not always lead to positive results. Although increasing online access to social security may increase its availability, built-in filters, perhaps resulting in algorithm bias, may negatively impact users. For example, Poland's public employment service, Publiczne Służby Zatrudnienia (PSZ), stopped using a controversial, automated scoring system for unemployment. The system's algorithm was used to "make life-changing decisions about what support individuals get based on their personal data and answers to interviews at job centres. Critics say the system is discriminatory, lacks transparency and infringes data protection rights."[412]

Digital self-realization implies digital space within which to self-realize. The specific rights that comprise this over-arching one, such as labor, education, and culture, exist within that larger digital space set aside for this larger purpose. In other words, Article 22's right provides not only a legal/philosophical foundation for those to occur, but also the context in which they occur. Commentary on the following sequence of UDHR articles explore these rights individually.

Article 23: Right to Work

With the ascendancy of the labor movement in the late 1940s when it was drafted, the right to work is one of the more expansively defined rights in the UDHR:

---

[411] Anriette Esterhuysen, *Why Focus on Economic, Social and Cultural Rights?*, *in* GLOBAL INFORMATION SOCIETY WATCH 2016: ECONOMIC, SOCIAL AND CULTURAL RIGHTS (ESCRS) AND THE INTERNET 6 (10th ed. 2016).

[412] Jędrzej Niklas, *Poland: Government to Scrap Controversial Unemployment Score System*, CTR. FOR INTERNET AND HUM. RTS. (Apr. 16, 2019), https://algorithmwatch.org/en/poland-government-to-scrap-controversial-unemployment-scoring-system/ [https://perma.cc/Z5R8-BFSL].

> (1) Everyone has the right to work, to free choice of employment, to just and favourable conditions of work and to protection against unemployment. (2) Everyone, without any discrimination, has the right to equal pay for equal work. (3) Everyone who works has the right to just and favourable remuneration ensuring for himself and his family an existence worthy of human dignity, and supplemented, if necessary, by other means of social protection. (4) Everyone has the right to form and to join trade unions for the protection of his interests.[413]

Prior to COVID-19, digital manifestation of the right to work mostly concerned development of the gig economy, outsourcing jobs, loss of work by humans to AI, the place of labor unions in the digital economy, employee digital privacy, and what was termed "teleworking." During and post-COVID, teleworking has overtaken all the rest thanks to the ubiquity of services such as Zoom, Teams, WebEx and others, although new AI issues loom on the horizon.

Development of the gig economy creates the environment within which these other concerns exist. The Internet has shaped labor in many ways, not least is how employers find workers and vice versa, how work is defined, and how work is carried out.[414] While the hiring process may be facilitated by Internet, so to may outsourcing—potentially endangering workers' jobs; taken on a mass scale, this dynamic could lead to "digital sweatshops" analogous to those in the physical world supporting textile industries.[415]

Digital outsourcing typically benefits the Global South, just as call centers traditionally have,[416] but clever employees can use this individually to their advantage. In 2013, for example, a code developer at Verizon, who

---

[413] UDHR, *supra* note 17, at art. 23.

[414] *See* Sonia Randhawa, *Labour, Migrant Communities and the Internet*, *in* GLOBAL INFORMATION SOCIETY WATCH 2016: ECONOMIC, SOCIAL AND CULTURAL RIGHTS (ESCRS) AND THE INTERNET, at 42 (2016).

[415] *See*Tessa Thomas & Korok Ray, *Online Outsourcing and the Future of Work*, 10 J. GLOB. RESP. 226, 232 (2018). However, the potential exists for firms in the Global South to "reverse outsource," which includes hiring specific skill sets more available in Global North economies. *See also* Elaine Pofeldt, *The New Outsourcing Hot Spots: More Developing Nation Firms Tap Workers in US, Canada, Europe*, CNBC (July 27, 2018), https://www.cnbc.com/2018/07/26/outsourcing-reverses-as-developing-nation-firms-hire-us-freelancers.html [https://perma.cc/Q844-JUVT].

[416] SIOU CHEW KUEK ET AL., WORLD BANK GROUP, THE GLOBAL OPPORTUNITY IN ONLINE OUTSOURCING 41–46 (2015).

earned several hundred thousand dollars, outsourced his assigned code work to be completed by a Chinese consulting firm for only fifty thousand dollars—a fraction of his salary.[417]

Relatedly, AI has already threatened job security,[418] quite literally amounting to the Internet *taking away* this human right. Kai-Fu Lee, an AI investor and formerly Google's top executive in China, predicts that "40 percent of the world's jobs will be lost to automation in the next 15 years."[419] If anything, COVID has accelerated this trend and, aside from routine maintenance, robots and AI driven systems aren't so affected by biological viruses.[420]

The International Labor Organization (ILO) offered the following definition of telework during the height of COVID: "Telework is defined as the use of information and communications technologies (ICTs), such as smartphones, tablets, laptops, and desktop computers, for work that is performed outside the employer's premises."[421] Unsurprisingly large numbers of non-essential employees began working from home during the pandemic; however, the ILO study flagged several labor issues that can arise from this dynamic, including an inability of the employer or employee to accurately track work time, benefits management, HR issues, and hidden overtime: "Teleworking, in general, can lead to longer working hours and also to working more during the evenings and the weekends," said the ILO[422]

Japan led the way in addressing some of these issues by loading avatars of individual workers into unique miniature robots that could then allow those workers to physically manifest themselves in the actual workplace. The ILO noted that:

---

[417] *See* Bill Chappell, *Outsourced: Employee Sends Own Job To China; Surfs Web*, NPR (Jan. 16, 2013), https://www.npr.org/sections/thetwo-way/2013/01/16/169528579/outsourced-employee-sends-own-job-to-china-surfs-web [https://perma.cc/7B4G-V3QY].

[418] Dan Bukszpan, *Here's How Amazon Robots Could Make the Deliveryman Extinct*, CNBC (Apr. 27, 2019), https://www.cnbc.com/2019/04/26/heres-how-amazon-robots-could-make-the-deliveryman-extinct.html [https://perma.cc/6R26-W6PK].

[419] *See* Tom Simonite, *Will AI Take Your Job—or Make It Better?*, WIRED (Dec. 16, 2019), https://www.wired.com/story/will-ai-take-your-job-or-make-it-better/ [https://perma.cc/82J2-2E5G].

[420] *See* Alana Semuels, *Millions of Americans Have Lost Jobs in the Pandemic—And Robots and AI Are Replacing Them Faster Than Ever*, TIME (Aug. 6, 2020), https://time.com/5876604/machines-jobs-coronavirus/ [https://perma.cc/6NCS-7J65].

[421] INT'L LAB. ORG., TELEWORKING DURING THE COVID-19 PANDEMIC AND BEYOND 1 (2020).

[422] *Id.* at 5.

> Using the avatar robots, remote workers can view their office and communicate with their colleagues. The roughly 20-cm-tall robots, with built-in camera, microphone and speakers, coupled with the "teleworking" application on a phone or iPad, is operated remotely by the teleworker and can be carried around by staff in the office, and can even attend meetings on behalf of remote employees.[423]

While returning to the workplace in this manner is a creative response to teleworking issues, the limited availability of the necessary technology to do so will prevent most countries from pursuing this option. More practical regulation, such as that undertaken by El Salvador simply transposing existing labor laws into digital space, may be a more useful path.[424]

Although COVID required humans to take the massive leap into online work, neither corporations nor governments shaped online work with any kind of intentionality—either by corporations or governments. Indeed, such rules and regulations that came about were in an effort to catch up to what had already occurred. Thus, very little uniformity, outside the uniformity imposed by available technology, exists for online work. In other words, everyone using the Zoom platform is in reality restricted by its technical abilities when using it—so there is situational uniformity, but rules vary widely among companies for things such as online billing, transactional engagement, information design and transfer, or cross-platform collaboration. The introduction and use of AI in this space complicates matters further and will be a key area to watch for more regulation in pursuit of Article 23's right to work online.

Article 24: Right to Rest and Leisure

The opposites of work, rest, and leisure are also important for full self-realization. Article 24's definition provides:

> Everyone has the right to rest and leisure, including reasonable limitation of working hours and periodic holidays with pay.[425]

Does this mean one's Internet human rights entitle them to pursue hobbies online such as genealogy research or photo scrapbooking in addition to

[423] *Id.* at 10.
[424] *Id.* at 23.
[425] UDHR, *supra* note 17, at art. 24.

playing online games? Of course. But it also means that access to virtual rest and leisure must achieve some norm of equality. Today, private interests completely control such access, and one must normally pay to pursue these activities.

In the work context, tracking programs are increasingly eliminating rest while at work. Newer versions of Apple products offer users the ability to turn on "screen time" that provides detailed activity logs of when and how often users are interacting with which programs and Internet sites—providing detailed activity logs. As businesses move to incorporate such systems into management practices, workers can lose their ability to take downtime between meetings or projects. One article notes that:

> These automated systems can detect inefficiencies that a human manager never would—a moment's downtime between calls, a habit of lingering at the coffee machine after finishing a task, a new route that, if all goes perfectly, could get a few more packages delivered in a day. But for workers, what look like inefficiencies to an algorithm were their last reserves of respite and autonomy, and as these little breaks and minor freedoms get optimized out, their jobs are becoming more intense, stressful, and dangerous.[426]

Rest and leisure are designed to keep workers healthy and productive. Eliminating it to boost higher short-term productivity can damage long-term productivity. As an Internet human right, there has been no discernable positive regulation in this area to date.

Article 25: Right to Adequate Standard of Living

Emerging from the devastation of the Second World War, the UDHR's drafters were keenly aware of the need to establish a minimum standard of living that was simultaneously aspirational. Thus, Article 25 states:

> (1) Everyone has the right to a standard of living adequate for the health and well-being of himself and of his family, including food, clothing, housing and medical care and necessary social services, and the right to security in the event of unemployment, sickness, disability, widowhood, old age or other lack of livelihood in

[426] Josh Dzieza, *How Hard Will the Robots Make Us Work?*, THE VERGE (Feb. 27, 2020), https://www.theverge.com/2020/2/27/21155254/automation-robots-unemployment-jobs-vs-human-google-amazon [https://perma.cc/JJ7Z-FZ4S].

> circumstances beyond his control. (2) Motherhood and childhood are entitled to special care and assistance. All children, whether born in or out of wedlock, shall enjoy the same social protection.[427]

Access to adequate healthcare is central to Article 25. In the United States, the Supreme Court has redefined a bedrock principle of female reproductive healthcare by overturning the storied *Roe v. Wade*[428]opinion in Dobbs v. Jackson.[429] Reproductive rights will now be regulated state by state, creating a patchwork quilt of healthcare availability for pregnant women, mirroring the international experience. The Internet can help educate women about what kind of healthcare is available across the United States just as it has done so for years internationally.[430]

In countries where social services have broken down completely, social media can be utilized by the population to support one another with information on where to find basic necessities such as food and medicine. In the wake of the economic meltdown in Venezuela, for example, social media was key to citizens providing themselves with an adequate social safety net.

> As economic mismanagement and political instability have pushed Venezuela deeper into crisis, digital and social media have become an increasingly important tool for daily life . . . . Posts like "I'll trade black beans for cornmeal" or "My father needs 40mg of losartan" have become a regular part of the social media landscape.[431]

In other cases, such technology has the potential to improve healthcare services in rural areas such as in Bangladesh, [432] or outlying islands such as

---

[427] UDHR, *supra* note 17, at art. 25.
[428] 410 U.S. 113 (1973).
[429] Dobbs v. Jackson Women's Health Org., 597 U.S. ___ , *5 (2022)..
[430] *See, e.g.*, Tarryn Booysen, *Role of the Internet in Realising Sexual and Reproductive Rights in Uganda: Interview with Allana Kembabazi*, GENDERIT.ORG (Dec. 6, 2016), https://genderit.org/articles/role-internet-realising-sexual-and-reproductive-rights-uganda-interview-allana-kembabazi [https://perma.cc/68F3-CSXA]..
[431] Rachelle Krygier, *Venezuela's Life-Saving Social Networks*, AMERICAS Q. (Aug. 23, 2016), https://www.americasquarterly.org/article/venezuelas-life-saving-social-networks/ [https://perma.cc/KT8V-E4MP].
[432]*See* Jasim Uddin et al., *Impact of Mobile Phone-based Technology to Improve Health, Population and Nutrition Services in Rural Bangladesh*, 17 BMC MED INFORMATICS & DECISION MAKING 101 (2017).

in the Philippines,[433] where an adequate standard of living is severely lacking. Utilizing the Internet to operationalize the leveling effect envisioned by Article 25 has, however, been sporadic and not an object of significant effort by governments or corporations. Thus, it remains an area ripe for positive regulation.

Article 26: Right to Education

The UDHR drafters to considered free compulsory elementary education a foundational base upon which all the other rights are built. Therefore, Article 26's mandate is quite detailed:

> (1) Everyone has the right to education. Education shall be free, at least in the elementary and fundamental stages. Elementary education shall be compulsory. Technical and professional education shall be made generally available and higher education shall be equally accessible to all on the basis of merit. (2) Education shall be directed to the full development of the human personality and to the strengthening of respect for human rights and fundamental freedoms. It shall promote understanding, tolerance and friendship among all nations, racial or religious groups, and shall further the activities of the United Nations for the maintenance of peace. (3) Parents have a prior right to choose the kind of education that shall be given to their children.[434]

Prior to COVID-19, states were already taking this right seriously, mandating education on how to use computers and the Internet for research and educational purposes within elementary school systems. Macedonia rolled out a "computer for every child program,"[435] Uruguay launched Plan Ceibal to promote universal remote English language teaching over the Internet to over 80,000 children in grades 4 to 6 in 568 state primary

---

[433] *See* Ashwin Chari, *In Support of UHC: Bringing Healthcare to Filipinos Through Telehealth*, PHILIPS (Feb. 20, 2020), https://www.philips.com.sg/a-w/about/news/archive/future-health-index/articles/20200220-bringing-healthcare-to-filipinos-through-telehealth.html [https://perma.cc/KH77-KKT2].

[434] UDHR, *supra* note 17, at art. 26.

[435] Vlado Apostolov, *Blank Screens: Lost Opportunities to Digitalize Education Haunt North Macedonia*, BALKAN INSIGHT (Oct. 26, 2020), https://balkaninsight.com/2020/10/26/blank-screens-lost-opportunities-to-digitalize-education-haunt-north-macedonia/ [https://perma.cc/X24B-DC5V].

schools,[436] and Kenya deployed a national education management information system to track testing, book distribution, attendance, and more through a central database that can help distribute resources on the ground.[437]

Yet not all aspects of education are easily translatable to digital form, or are at least not as readily accepted. For example, use of e-textbooks, which are not widely accepted by the students who are supposed to use them.[438] Accounting for societal differences in educational coverage, educational opportunities should be more uniform. With respect to the content of this Internet human right, "the right to education has four 'interrelated and essential features': availability, accessibility, acceptability and adaptability . . . these features have implications for the internet and related technologies."[439] Connectivity and net neutrality are both in play as key principles animating this digital right.

What was termed "distance-learning" prior to COVID became the norm during the pandemic, thanks to widely available and easily useable digital group assembly platforms such as Zoom. According to UNICEF, once the pandemic globalized, "a majority of countries . . . announced the temporary closure of schools, impacting more than 91 per cent of students worldwide—around 1.6 billion children and young people."[440] However, just because children were unable to attend school, their human right to education did not disappear.

Countries scrambled to move entire school systems to online platforms. Yet despite these efforts, an estimated 364 million children remained unable

---

[436] *Plan Ceibal: Remote Teaching into Uruguayan Public Schools*, BRITISH COUNCIL (2022), https://www.britishcouncil.uy/en/programmes/education/ceibal-en-ingles. [https://perma.cc/4P59-UC93].

[437] *Kenya: Investing in Education for a Better Future*, GPE (Mar. 2023), https://www.globalpartnership.org/results/stories-of-change/kenya-investing-education-better-future [https://perma.cc/8HQ5-WEGX].

[438] *Teaching and Learning with eTextbooks*, UNIV. OF IOWA OFF. OF TEACHING, LEARNING & TECH. (2018), https://teach.uiowa.edu/teaching-and-learning-etextbooks [https://perma.cc/BV55-288K].

[439] GLOB. INFO. SOCIETY WATCH, THE RIGHT TO EDUCATIONAL RESOURCES AND THE INTERNET 27 (2016), https://giswatch.org/en/economic-social-and-cultural-rights-escrs/right-educational-resources-and-internet.

[440] Jason Miks & John McIlwaine, *Keeping the World's Children Learning Through COVID-19*, UNICEF (Apr. 2020), https://www.unicef.org/coronavirus/keeping-worlds-children-learning-through-covid-19 [https://perma.cc/3QPW-XS28].

to attend school remotely due to lack of connectivity.[441] As with teleworking in Article 23's right to work, the right to education may exist post-COVID in somewhat of a hybridized format with remote education more prevalent in the upper reaches of the educational spectrum (secondary schools) and less so at the primary levels. However, regulation and enforcement will continue to be an obligation of state educational authorities per domestic compulsory education requirements.

Just as COVID pushed Article 23's right to work online, it pushed Article 26's right to education online. Mandatory K-12 public education schemes were delivered unevenly at best, but the effort was definitely there with respect to adapting synchronous teacher-student contact with asynchronous workshops and homework projects. Although not ideal, the 18-month global experiment in online education proved that this right could exist online in a meaningful way nonetheless.

With that proof of concept in hand, opportunities now exist for school systems to take advantage of offering more intentional e-learning possibilities. For example, in North America, once regular school got underway post-COVID, traditional "snow days" for bad weather which used to result in free days at home for students were replaced in many school systems with e-learning days so that the classes and calendars could remain on schedule for the term. Such adaptations can be improved and extended.

Article 27: Right to Cultural, Artistic and Scientific Life

Enrichment of the human experience is the focus on UDHR Article 27, which states:

> (1) Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits. (2) Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.[442]

That enriched human experience is secured in the first part via access to cultural and scientific heritage and in the second part via the protection accorded to artists and scientists for their creations.

---

[441] Henrietta Fore, *Without Internet, 364 Million Children are Falling Behind*, CNN BUSINESS (Apr. 4, 2019), https://www.cnn.com/2019/04/04/perspectives/unicef-schools-internet-access/index.html [https://perma.cc/F3EK-Z6VA].

[442] UDRH, *supra* note 17, at art. 27.

Digitally, this could translate to remote access to museums, planetariums, zoos, and the like as well as intellectual property protection. Some private museums charge admission for digital entry, but most public ones do not. The digital experience typically takes the form of a three-dimensional immersion. Absent widely available VR equipment, this is probably as close as one can get to visiting the site physically. However, the experience has not been limited to museums; using now ubiquitous drone technology, students and the public can visit archeological sites in the field or geologically interesting sites such as volcanoes, forests, gorges, and glaciers. There is no state regulation to date in this field.

For scientific knowledge, dispersal through open-access digital repositories is how Article 27 manifests.[443] A balance has been struck in cyberspace between electronic journals that charge for access to their content and platforms that freely post all content—the debate currently centering on use of funding for subscriptions to support further research that may ostensibly be undermined by too much free access.

The main form of regulation that occurs with respect to Internet human rights and Article 27 is intellectual property protection – especially at the international level. The TRIPS agreement under the World Trade Organization is the leading international legal regime protecting those digital human rights.[444] Articles 41 through 46 establish the enforcement framework required of member states and have been used in the digital context to secure creators' intellectual property rights in cyberspace.[445]

Thus, this aspect of Article 27 is one instance of a UDHR right manifesting, being codified (by analogy) and regulated, and becoming enforceable as a matter of international law. Unlike the enforceability of Article 12's privacy right as the E.U.'s right to be forgotten—which depends upon corporate enforcement by Google, enforcement here is achieved by states complying with their international legal obligations.

---

[443] Éanna Kelly, *EU and National Funders Launch Plan for Free and Immediate Open Access to Journals*, SCI. BUS. (Sept. 4, 2018), https://sciencebusiness.net/news/eu-and-national-funders-launch-plan-free-and-immediate-open-access-journals [https://perma.cc/63DN-QKS4].

[444] Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994).

[445] *Id.* at art. 41–46; *see also* Antony Taubman, *TRIPS Encounters the Internet: An Analogue Treaty in a Digital Age, or the First Trade 2.0 Agreement*, *in* TRADE GOVERNANCE IN THE DIGITAL AGE (Butti & Cottier, eds. 2015).

The next horizon for litigation in this area is likely to concern derivative intellectual property rights due to the propensity of the Internet to enable easy downloading and manipulation of creative works.

> In many cases in the digital world, new works are created drawing on the works of others. Digital technology makes it easy to copy and modify parts of existing content and to mix them to create new content. Harvard law professor Lawrence Lessig called it a "remix" or "read-write" culture.[446]

The Internet has become an incredible vehicle for delivering creative work to ever wider audiences. As such, it has also become an incredible risk for creative artists to lose their works to intellectual property theft. Although robust domestic and international legal regimes exist to protect these rights in the physical world, these regimes must go further into online transference to bring Article 27's right to culture, artistic, and scientific life to full effect.

Article 28: Right to Social Order

Enforceability of human rights is the focus on Article 28, which provides:

> Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized.[447]

Within states, it is the responsibility of the central government to enforce international law. What form this enforcement takes and which components of the government actually accomplish this task vary widely—often depending on whether the particular state is an open democracy or a dictatorship. With respect to Internet human rights, governments sometimes create regulatory entities or ministries that have some or all powers in this regard. The United States approaches this task very loosely through the Federal Communications Commission (FCC). France divides its Internet administrative roles into two spheres: the Autorité de Régulation des Communications Électroniques et des Postes (ARCEP), which regulates the nuts and bolts and technical aspects of the Internet, and the Commission

---

[446] GLOB. INFO. SOCIETY WATCH, , REPUBLIC OF KOREA: ECONOMIC, SOCIAL AND CULTURAL RIGHTS AND THE INTERNET 140 (2016).
[447] UDHR, *supra* note 17, at art. 28.

Nationale de l'Informatique et des Libertés (CNIL), an independent agency which actually polices the Internet.

CNIL takes a very aggressive stance on data protection enforcement. Recent actions have included compliance orders and large sanctions against companies like Google, Microsoft, and Facebook. CNIL is backed by a strong legal framework, the most recent legislation of which, apart from the E.U.'s General Data Protection Regulation is the French Digital Republic Act of 2016.[448] The Act "created new data protection rights, such as (1) the right for individuals to give instructions relating to the storage, erasure and disclosure of their personal data after their death, (2) the right to be forgotten for minors and (3) the possibility to exercise data protection rights by electronic means. This legislation strengthens the transparency requirements and increases the maximum level of fines from €150,000 to €3 million for data protection infringements."[449]

For autocratic regimes, agencies tasked with regulating the Internet are often no more than censorship arms of the regime, and can in fact be double-tasked as surveillance mechanisms.[450] Internet shut-downs during political uprisings challenging such regimes are common.

Because of vast differences in regulatory approaches to the Internet within states, it is doubtful that reliance on domestic enforcement would yield much consistency. Of course, this is the same problem with respect to international law generally and human rights in particular. Yet absent a robust international enforcement model, the domestic model—incoherent and inconsistent as it may be—is currently the only option available.

In the end, enforcement arrives in two stripes in the case of Internet human rights: government enforcement for those rights existing in cyberspace controlled by governments, and enforcement by Big Tech for those rights existing in cyberspace controlled by corporations. In the first case, consistent and even-handed enforcement are hallmarks of modern democracies; in the second instance, uneven and arbitrary enforcement are

---

[448] Loi n 2016-1321 du 7 Octobre 2016 Pour une République Numérique (1) [Law 2016-1321 of October 7, 2016 For a Digital Republic (1)], J. OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE 0235 at 1 (Oct. 8, 2016).

[449] *CNIL Unveils 2017 Inspection Program and 2016 Annual Activity Report*, PRIV. & INFO. SEC, L. BLOG, (Mar. 29, 2017), https://www.huntonprivacyblog.com/2017/03/29/cnil-unveils-2017-inspection-program-2016-annual-activity-report/ [https://perma.cc/VP5Y-JJX4].

[450] *See, e.g.*, Justin Sherman, *Russia's Internet Censor is Also a Surveillance Machine*, COUNCIL ON FOREIGN RELS. (Sept. 28, 2022), https://www.cfr.org/blog/russias-internet-censor-also-surveillance-machine, [https://perma.cc/PJ2C-XXKP].

likely across corporate spheres in the absence of baseline rules promulgated by states, as evinced by the drama surrounding Twitter's recent acquisition by Elon Musk concerning whom he would allow or not allow to use the platform.

Article 29: Duty to Your Community

Self-restraint is the premise of Article 29, which provides:

> (1) Everyone has duties to the community in which alone the free and full development of his personality is possible. (2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society. (3) These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations.[451]

Self-restraint on the Internet entails avoidance of many of the behaviors that are becoming criminalized and discussed above in various articles, including cyber-bullying, hacking, identity theft, cyber-stalking, digital harassment, etcetera. The general welfare of a democratic society becomes, in cyberspace, the general welfare of the digital world available to all of us on the Internet. Care for that environment is incumbent on everyone, but this obligation should not be limited to natural persons.

Just as in the physical world, corporations walk the landscape in the digital world. However, the powers of these legal persons are greatly enhanced when in their digital form. Not only do some of the largest and wealthiest corporations provide the platforms on which we all engage one another, they also control the terms of that engagement via their terms of service, which they can change at any time.[452] Leaving enforcement of many Internet human rights to companies could be the Achilles' heel in this entire paradigm. Yet few alternatives are available. Consequently, social pressure on those corporations to comply with the Internet human right of sharing a common duty to our community is all the more important.

---

[451] UDHR, *supra* note 17, at art. 29.

[452] Luca Belli & Jamila Venturini, *Private Ordering and the Rise of Terms of Service as Cyber-Regulation*, 5 INTERNET POL'Y REV. 1, 4 (2016).

Beyond the social responsibility paradigm that companies began incorporating into their business practices in the early 2000's,[453] increasingly more so now with the rise in importance of ESG,[454] Article 29 could be viewed as a duty incumbent on corporations with a significant Internet presence. Just as a court determined that Google essentially had a duty to its community to process erasure requests from search results, a court could similarly find that Twitter or Facebook has a duty to its community to scrub hate speech and lies from their platforms in order to ensure Article 29's promise. Consequently, Article 29 could in fact serve a much a larger role in defining corporate Internet behavior than might appear at first glance. That, however, is a path for future litigation.

Article 30: Rights are Inalienable

Once vested, human rights cannot be taken away. Article 30 completes the UDHR's vision by stating:

> Nothing in this Declaration may be interpreted as implying for any State, group or person any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms set forth herein.[455]

Taken to the Internet, the digital version of human rights should not be abrogated once secured. The object of the matrix offered in this paper is to determine which human rights are blossoming into digital reality. A few have completed their journey, albeit sometimes in different forms, many are in progress, and several still have yet to begin. Enforcement across Internet human rights is also inconsistent and, in the case of corporate enforcers, unsecure. Yet the principle must be nevertheless supported that once these rights blink into existence on the Internet, they must be secured.

However, this raises a question of the durability of the legal instrument that contains them. For example, such rights can be included in treaties, constitutions, statutes, administrative regulations, contracts, or mandated by court judgments. Each of these vehicles feature vastly different methods for

---

[453] *See generally* Adam Lindgreen & Valérie Swaen, *Corporate Social Responsibility*, 12 INT'L J. MGMT. REVS. 1 (20010).
[454] *See* Michael J. Kelly, *ESG: The 5th Element of Corporate Risk Assessment*, 2022 MICH. ST. L. REV. 811 (2022).
[455] UDHR, *supra* note 17, at art. 30.

adjustment that could lead abrogation. Treaties are relatively easy for states to withdraw from given proper notice; constitutions typically require difficult amendment procedures; statutes can be repealed; regulations can be simply withdrawn; contracts can be renegotiated or terms of service may be applied; and, court judgments can be overturned. Thus, the impediment associated with altering the deal secured by the legal instrument may in fact be determinative of whether Article 30's rights securitization promise is met.

Conclusion

What human rights follow us into digital space? As the time humans spend in that space increases year by year, this question takes on more salience. Although this paper's matrix tracks the current progress of that migration, it is only a starting point. Further monitoring will be required to map additional progress, analyze adaptations that occur during transference, and identify new gaps or stalled progress that can create space for negative regulation by states or corporations. Yet, as the first legal mapping project of its kind, we hope this becomes a useful tool for the human rights community as well as for digital space regulators.

Corporate definition and enforcement of Internet human rights opens up an entirely new regulatory world—one in which we find ourselves daily, either complying with or flouting corporations' terms of service. Whether mandated by a court, as with Google and the right to be forgotten, or simply filling a vacuum, as with free expression on Twitter, much more intentionality and policy discussion is needed. Meanwhile, corporate involvement in effectuating such rights is at least now being tracked in a holistic manner.

The person in which an Internet human right vests, is, for now, still the physical being at the keyboard or attached to the virtual reality device. While some argue for the digital manifestations of people to be the actual rights-holder, the law has simply not caught up to such a notion. Certainly, as physical people pass away, their digital forms may linger on for some time in games, on social media, and in other digital venues.[456] Does the Internet human right die with the physical person or somehow linger on as well? Thus, questions of vestment and duration also require more discussion.

Finally, unanimity in Western democracies regarding universal connectivity has not been followed with similar unity on net neutrality policy.

---

[456] Maria Perrone, *What Happens When We Die: Estate Planning of Digital Assets*, 21 COMMON L. CONSPECTUS 185, 185–86 (2012).

Neither point has become fully realized in non-Western societies. Without these precursor core rights secured, many Internet human rights cannot digitally gel. In fact, connection itself may be something people are willing to periodically eschew in order to re-center themselves in the physical realm. Ironically, the final edits for this paper were undertaken at Lyceum Pub – "a digital de-tox" establishment on London's Strand, devoid of Internet service. Consequently, no Internet human rights were at stake in our conclusion. Bringing Hamlet's query forward by 400 years: "To connect, or not to connect? That is the question." Turns out, it matters quite a lot how you answer.

Appendix

Digital Human Rights Reports by United Nations Special Rapporteurs:

- Frank LaRue, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, GA, HRC, Report, 17th Sess., U.N. Doc. A/HRC/17/27 (May 16, 2011).

- David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, GA, HRC, Report, 29th Sess., U.N. Doc. A/HRC/28/32 (May 22, 2015).

- Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Int'l Law Comm'n, U.N. Doc. A/HRC/38/35 (Apr. 6, 2018).

- Clément Nyaletsossi Voule, Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and Association, GA, HRC, Report at ¶ 10, 41st Sess., U.N. Doc. A/HRC/41/41 (May 17, 2019).