Human Rights, the United Nations, and Digital Technologies: Configuring Human Rights in Software Code

by

Timothy S. Reiniger, Esq. and Stephen Mason

This submission is in response to the June 10, 2019 call by the United Nations Secretary-General's High-Level Panel on Digital Cooperation for assistance in determining the application of human rights principles on digital technologies.[1] In the global network information society, it is crucially important that individuals be given the juridical means to enforce their human rights in personal information. We conclude that the human rights tradition, as embodied in the United Nations Declaration of Human Rights (UDHR), is currently unrealized in the machine-space of the digital environment, which defaults to being authoritarian.[2] After discussing the UDHR articles that are most pertinent, we present examples of emerging approaches that may serve as functional mechanisms for protecting and enforcing human rights in the machine-mediated age governed by software code.[3]

Human Rights and Digital Technologies

To his Excellency the Honorable António Manuel de Oliveira Guterres, Secretary-General of the United Nations. (September 11, 2019.)

I. Introductory Observations: Human Rights in the Machine-Mediated Age Governed by Software Code

A. Digital Technologies and the Machine-Mediated Age Governed by Software Code

---

[1] *See* "The Age of Digital Interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation," (June 2019), *available at* https://digitalcooperation.org/. In particular, this submission responds to recommendations 3A and 3C, found on pages 38-9 of the Report. Note that neither the Report nor this submission addresses the matter of applying the UDHR articles to the fields of human genetics and bioengineering. The authors of this submission urge the UN Secretary General to consider organizing a high-level panel to discuss this as well. For an introduction to the issues raised by software code in this context, see JEREMY RIFKIN, THE BIOTECH CENTURY: HARNESSING THE GENE AND REMAKING THE WORLD(1998) (describing the application of cybernetics to processes in living organisms) and BILL MCKIBBEN, ENOUGH: STAYING HUMAN IN AN ENGINEERED AGE (2003).

[2] The UDHR is available at https://www.un.org/en/universal-declaration-human-rights/. The authors note that the principles of the UDHR have been incorporated in a wide variety of United Nations documents, including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social, and Cultural Rights.

[3] In the context of this submission, the authors note that software code is colloquially called "artificial intelligence" and David Harel, in COMPUTERS LTD. WHAT THEY REALLY CAN'T DO 194 (2000), refers to "algorithmic intelligence."

1. We now live in an information society or, to put it more accurately, we live in a machine-mediated age governed by software code.[4] The network communication of one item of software with another item of software governs much of what we do when interacting with machines controlled by software. Therefore, a critically important issue is the recognition and enforceability of human rights that we can expect when using machines and digital identities that are controlled by software.[5]

2. Many individuals experience serious disruption in their lives because an identity thief has used their digital identity and additional personal identifying information and attributes contained in numerous network databases (such as government service records; bank accounts; credit bureaus; and credit card data) to secure unauthorized network access to steal from others in the name of the innocent person, creating financial losses that are difficult to resolve.[6]

3. The reliance upon software in the information age has challenged legal systems to understand how to assess the trust placed in machines controlled by software, and how to determine and prove that a responsible *person* or *persons* may or may not be responsible for the communications between the machines.[7]

4. Corporate and governmental surveillance of the lives of ordinary people is now ubiquitous.[8] Yet, there is no consensus on whether informational privacy is a human right.[9]

---

[4] The influence of software code, network architectures, technological capabilities, system design choices, and machine-mediated environments on creating information use rules and regulating behavior in cyberspace has been referenced as 'code is law' in LAWRENCE LESSIG, CODE VERSION 2.0 (2008) and as 'Lex Informatica' by Joel R. Reidenberg in *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553 (1998). For purposes of this article, we give the term 'software' this broad meaning. *See also*, Dan L. Burk, *Lex Genetica: The law and ethics of programming biological code*, 4 ETHICS AND INFORMATION TECHNOLOGY 109, 112 −121 (2002), in which the application of Lex Informatica technological and system design policy approaches for regulating human behavior are applied in the context of programmable biological code.

[5] A growing number of national authorities are now issuing identity credentials in digital form. Information on the current status by country is available at https://www.worldprivacyforum.org/2017/07/national-ids-around-the-world/.

[6] This topic is discussed in detail in Nicholas Bohm and Stephen Mason, *Identity and its verification*, COMPUTER LAW & SECURITY REVIEW, Vol. 26, No. 1, 43 – 51 (2010).

[7] This topic is discussed in detail in Stephen Mason and Timothy Reiniger, *'Trust' Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog?* 22 COMPUTER LAW & SECURITY REVIEW, Issue 5, 135-48 (2015).

[8] For a representative discussion, see SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

[9] *See* Stephen Mason, *The Internet and Privacy: Some Consideration*, 21 COMPUTER LAW & SECURITY REVIEW, Issue 3, 68-84 (2015). Nor is there international consensus on the concept of privacy. *Id*. at 74.

5. There is no consensus on whether access relations in the networked environment is a human right.[10]

B. Conditions for the Recognition and Enforceability of Human Rights

6. The origins of our current understanding of human rights traces to the twelfth-century recognition of humans as holders of inherent natural rights and the adaptations of these concepts to the conditions in subsequent centuries.[11]

7. Historically, the recognition and enforceability of natural or human rights rests on three fundamental principles: a) human beings with inherent rational and moral faculties and powers, b) human beings with free will to act, and c) human beings with subjective rights or authority to act, including active claim rights.[12]

8. Human rights historically have been shaped by responses to abuses by anonymous corporate structures including governments, religious institutions, and business corporations.[13] Systems and automated processes, by themselves, do not command the trust of users.[14]

---

[10] JEREMY RIFKIN, THE AGE OF ACCESS 237-39 (2000) (discussing the merits of making access to networks and information a right in view of the growth of commoditized internet and mobile telephone access). Arguing in support of an access right to the internet is the Global Citizenship Commission in "The Universal Declaration of Human Rights in the 21st Century: A Living Document in a Changing World (chaired by Gordon Brown) (NYU Institute for Advanced Study, 2016), *available at* *https://www.openbookpublishers.com/reader/467#page/2/mode/2up*.

[11] BRIAN TIERNEY, THE IDEA OF NATURAL RIGHTS 43-77 (1997). RICHARD TUCK, NATURAL RIGHTS THEORIES: THEIR ORIGIN AND DEVELOPMENT 13-31 (1979). *See also*, HAROLD BERMAN, LAW AND REVOLUTION 351 (1983).

[12] Tierney, *supra* note 11, at 44-8, 64-9, 242-9, and 343-8. *See also* Brian Tierney, *Historical Roots of Modern Rights: Before Locke and After,* 3 AVE MARIA L. REV. 23 (2005); Brian Tierney, *The Idea of Natural Rights—Origins and Persistence*, 2 NORTHWESTERN J. INT'L HUMAN RIGHTS 4-8 (2004) and Charles J. Reid, Jr., *The Canonistic Contribution to the Western Rights Tradition: An Historical Inquiry*, 33 B.C.L REV. 37 (1991). Note that modern physics now lends support to the concept of free will. RICHARD A. MULLER, NOW: THE PHYSICS OF TIME 10 (2016) ("Despite arguments from classical philosophers, we now know that free will is compatible with physics; those who argue otherwise are making a case based on the religion of physicalism. We can influence the future using not only scientific but also nonphysics knowledge (empathy, virtue, ethics, fairness, justice) to guide the flow of entropy to bring about a strengthening of civilization or its destruction.") With respect to juridical claim rights, see A.W. BRIAN SIMPSON, HUMAN RIGHTS AND THE END OF EMPIRE: BRITAIN AND THE GENESIS OF THE EUROPEAN CONVENTION 3-4 (2001) (noting that an outstanding feature of the European Convention is that it gives individuals standing to initiate private juridical complaints.)

[13] For a representative discussion of human rights abuses suffered by indigenous peoples in South and Central America and the Caribbean, see BARTOLOME DE LAS CASAS, A SHORT ACCOUNT OF THE DESTRUCTION OF THE INDIES (Penguin Books 1992) (estimating that 10-15 million indigenous persons lost their lives under great suffering, including torture).

> And so blinded by ambition and driven by greed are the devils who advocate such treatment of these people that they cannot see that, when their victims come to obey under duress this foreign overlord and publicly recognize his authority over them, simply because of their fear of what will happen to them if they do not, such a recognition of suzerainty has no standing in law whatever, any such prerogative obtained by menaces from any people anywhere in the world being invalid. In practice, the only rights these perfidious crusaders have earned which can be upheld in human, divine, or natural law are the right to eternal damnation and the right to answer for the offenses and harm they have done….

9. Digital technologies by themselves do not threaten human rights. Instead, the threat comes from human beings.[15]

10. Digital technology development reflects the emerging needs of society as it is organized.[16]

11. In its current form, the UNDHR can be applied effectively to enable the recognition and enforcement of human rights in the global digital network-based environment.

II. Human Rights and Digital Technologies: The Pertinent Articles in the United Nations Declaration of Human Rights

A. Article 1

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.

12. Subjective rights are those that are inherent to each person and are inseparably part of each personality.[17] Therefore, such subjective rights exist whether or not

---

Id. at 53-4. For a discussion of the Second World War origins of the UDHR, see GEOFFREY ROBERTSON, CRIMES AGAINST HUMANITY: THE STRUGGLE FOR GLOBAL JUSTICE 26-34 (1999).

[14] JOSEPH VINING, THE AUTHORITATIVE AND THE AUTHORITARIAN 25, 46 (1986). *See also* VACLAV HAVEL, DISTURBING THE PEACE: A CONVERSATION WITH KAREL HVÍŽĎALA 10, 195–96 (Paul Wilson trans., 1990) (discussing the cause of the global trust crisis as the…"conflict between an impersonal, anonymous, irresponsible, and uncontrollable juggernaut of power (the power of 'mega machinery') and the elemental and original interests of man as a concrete individual.").

[15] NORBERT WIENER, THE HUMAN USE OF HUMAN BEINGS: CYBERNETICS AND SOCIETY 181 (1954) (the real danger is that "…such machines, though helpless by themselves, may be used by a human being or a block of human beings to increase their control over the rest of the human race or that political leaders may attempt to control their populations by means not of machines themselves but through political techniques as narrow and indifferent to human possibility as if they had, in fact, been conceived mechanically."). *See also* ALDOUS HUXLEY, BRAVE NEW WORLD xiv (Forward) (1932) ("Indeed, unless we choose to decentralize and to use applied science, not as the end to which human beings are to be made the means, but as the means to producing a race of free individuals, we have only two alternatives to choose from: either a number of national, militarized totalitarianisms…or else one supra-national totalitarianism…."); Havel, *supra* note 14, at 13 ("The most important thing is that man should be the measure of all structures, including economic structures, and not that man be made to measure for those structures.").

[16] MARK KURLANSKY, PAPER: PAGING THROUGH HISTORY xvii (2016) ("Technology is only a facilitator. Society changes, and that change creates new needs. That is why technology is brought in. The only way to stop the technology would be to reverse the changes in the society.").

[17] Tierney, *supra* note 11, at 20-30, 42-57, 64-8, and 88. "The one necessary basis for a theory of human rights is a belief in the value and dignity of human life." *Id.* at 247. For an illustrative modern application, see the *West German Abortion Decision*, 9 THE JOHN MARSHALL JOURNAL OF PRACTICE AND PROCEDURE 605, 662 (1976)) (translation by Robert E. Jonas and John D. Gorby) ("Underlying the Basic Law are principles for the structuring of the state that may be understood only in light of the historical experience and the spiritual-moral confrontation with the previous system of National Socialism. In opposition to the omnipotence of the totalitarian state which claimed for itself limitless dominion over all areas of social life and which, in the prosecution of its goals of state, consideration for the life of the individual fundamentally meant nothing, the Basic Law of the Federal Republic of

contained in national legislation.[18]

13. An essential basis for the recognition and enforceability of human rights in the global information society is the authentication of legal identity.[19] Yet we lack a common global method for enabling and recognizing legal identities in the digital environment.[20]

14. The network-based economy and systems each require trust in the capability to identify and authenticate individuals who seek to obtain access to networks, share information, and sign documents.

15. Both public and private sector participants in the identity ecosystem recognize that open markets for the exchange of identity information are essential to trusted online access to networks. Nevertheless, current internet identity markets are dominated by identity management systems in which users have little or no control over their data and little to no visibility as to where their data flows and how it is used.

16. The rise of the digital network-based information economy, and the cybernetic theories upon which it is based, has produced identity deficit or increased absence of the person.[21] For law, cybernetics[22] governance principles and computing machines

---

Germany has erected an order bound together by values which places the individual human being and his dignity at the focal point of all of its ordinances.").

[18] We note there may be legal uncertainty as to whether all Articles in the UDHR are recognized as being within the body of international law. For a discussion of this legal issue, see Robertson, *supra* note 13,.at 80-92.

[19] Patrick McKenna, *The Probative value of digital certificates: Information Assurance is critical to e-Identity Assurance*, 1 DIGITAL EVIDENCE AND ELECTRONIC SIGNATURE LAW REVIEW 59 (2004) ("Trust belongs to people and organization, rather than technology."); ANDREW MURRAY, INFORMATION TECHNOLOGY LAW: THE LAW AND SOCIETY 486 (2013) ("[O]ne of the effects of the information society is a divorce of identity from the person. Basically this means that with more of our everyday lives being ordered or even accessed via an internet connection, we increasingly use proxy data to identify who we are."). For a discussion of how the individual is disembodied in cyberspace (also understood as the 'space' or network in which machine-mediated communication occurs) *see* DOUGLAS GROOTHUIS, THE SOUL IN CYBERSPACE 37 (1997) (Machine-mediated identity is a "medium for disembodiment.").

[20] Currently, over one billion people in the world lack a legal identity. For information on the lack of civil birth registration in many countries, see, by way of example, https://www.unicef.org/rosa/what-we-do/child-protection/civil-registration. A major challenge has been the lack of reliable means by which to identify persons in rural areas of many developing countries. To address this, efforts are being launched in Haiti by the Episcopal Diocese of Maine (a member of the Anglican Communion) to leverage the rural presence and vital information collected by NGOs in the form of faith-based organizations.

[21] *See, e.g.*, Havel, *supra* note 14, at 195–96 (referencing "identity that is decaying, collapsing, dissipating, vanishing" in the face of "impersonal, anonymous, irresponsible" power); GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE 92 (2008) ("Fundamental to any discussion about proof of digital identity is an understanding that information systems have no intrinsic way of knowing the identity of entities that participate in the systems' reading and writing games."); JOSEPH VINING, FROM NEWTON'S SLEEP 248 (1995) ("[T]he personal disappears in process and system.").

[22] Wiener *supra* note 15, at 15 and 27 (defining cybernetics as the study of messages to explain purposive behavior in machines and how they regulate themselves in changing environments and systems).

have caused profound policy crises related to authentication, authenticity, and authority. Specifically, cybernetics raises important legal considerations with respect to the manner in which information and actions are linked to persons, authenticity is proven, and responsibility is determined in systems.[23]

17. Digital technologies order systems by means of quantifying life into bits of information or amounts of entropy.[24] But human identity needs to be approached holistically and not analytically.[25] A holistic strategy identifies a person by understanding his or her relationships and functions within a larger context or community. An analytical strategy identifies a person through a reductionist method of labeling constitutive attributes or parts.

18. Recognition of the person results in greater emphasis on human choice, free will, and intent.[26]

B. Article 6

Everyone has the right to recognition everywhere as a person before the law.

19. With automation and artificial intelligence, the legal responsibility for the consequences of software-related failures is obscured. With respect to machines controlled by software, we do not have direct evidence of the identity of a responsible

---

[23] *Id.* at 17–18, 25–27 (suggesting that cybernetics reduces all activity to processes, which consist of two ingredients: information and feedback). *See also* PETER F. DRUCKER, THE AGE OF DISCONTINUITY: GUIDELINES TO OUR CHANGING SOCIETY 38 (1969) ("Underlying [the information industry] is a new perception: the perception of 'systems.'").

[24] WIENER, *supra* note 15, at 21–27 (describing the use of machines and feedback systems to stabilize performance and control the entropic tendency toward disorganization in nature and society). *See also* VINING, *supra* note 21, at 37–41.

> All in this view of the world and ourselves flows from the reduction of all to process and pattern, the first step in scientific thinking, and from the associated reduction of saying to doing. Everything depends upon these two assumptions, that the person or self can be collapsed into pattern and process, and that saying can be equated to doing or "behavior," permitting observation from the outside.

Id. at 41.

[25] PETER DRUCKER, THE NEW REALITIES 262 (1989) ("And biological process is not analytical. In a mechanical phenomenon the whole is equal to the sum of its parts and therefore capable of being understood by analysis. Biological phenomena are however "wholes." They are different from the sum of their parts.").

[26] Warren Weaver, *The Mathematics of Communication*, 181 SCI. AM. 11, 13 (1949) ("Information is . . . a measure of one's freedom of choice in selecting a message. The greater this freedom of choice, and hence the greater the information, the greater is the uncertainty that the message actually is some particular one. Thus greater freedom of choice, greater uncertainty, greater information go hand in hand."). S*ee generally* VINING, *supra* note 21, at 281 ("Against the constant fading of the conditions of authority is what comes from law that pushes toward the personal and a context of decision making in which the personal can be recognized, recognition of the personal being the only entry to the experience of authority.").

person who actually controls its use.[27] In this respect, the comment by Pierre de Latil that 'The machine will never be able to tell who directs its activity' is highly apposite.[28]

20. Automatons and robots have no capability for consciousness or conscious agency.[29]

21. Machine or system-made evidence should be neither automatically deemed more reliable than human testimony, nor given evidentiary presumptions.[30] "One presumption that may apply to computers is the presumption that a machine is presumed to be in working order. In the context of digital evidence, however, it is pertinent to be aware of the imperfections inherent in the way computers function, and how digital evidence is prone to alteration. Evidence derived from a computer must be admissible, authentic, accurate and complete in the same way as any other form of evidence."[31]

22. Within the context of litigation, a bank, for example, will make every effort to refrain from revealing evidence of its software systems and the rationale for its reasoning. In so doing, the bank will usually ask an adjudicator to accept their assurances without providing evidence to sustain their claims, and judges will accept such assurances in the absence of any evidence.[32] This illustrates the comment by

---

[27] For a discussion about how the examples of electronic signatures and networked communications are challenged by a lack of evidence in proving who clicked the button or caused the particular signature to be made, *see* STEPHEN MASON, ELECTRONIC SIGNATURES IN LAW, 189 (Institute of Advanced Legal Studies, 4th edn, 2016). *See also* Vining, *supra* note 21, at 281 (1995) ("And the central concern of law, atheoretical, pretheoretical, is then connection of value and responsible mind, for value not connected by mind to responsible belief is mirage, nothing, vanishing when questioned or sought.").

[28] PIERRE DE LATIL, THINKING BY MACHINE: A STUDY OF CYBERNETICS 342 (1957).

[29] Stephen Mason, *Artificial Intelligence: Oh Really? And Why Judges and Lawyers are Central to the Way we Live Now – But they Don't Know it*, 23 COMPUTER LAW & SECURITY REVIEW, Issue 8, 213-5 (2017) ("Software code injures and kills people.").

[30] Mason, *supra* note 27, at 386. For a detailed discussion on the presumption that computers are reliable and judicial notice in respect of software, and why such a presumption is not appropriate, see STEPHEN MASON AND DANIEL SENG, editors, ELECTRONIC EVIDENCE (Institute of Advanced Legal Studies, 4th edn, 2017), chapter 6.

[31] Mason, *supra* note 27, at 385-86.

[32] For an example of the assurances accepted by a judge without any evidence, see the Norwegian case of Bernt Petter Jørgensen v DnB NOR Bank ASA, Trondheim District Court, 24 September 2004, 9 DIGITAL EVIDENCE AND ELECTRONIC SIGNATURE LAW REV 117 – 123 (2012); Maryke Silalahi Nuth, *Unauthorized use of bank cards with or without the PIN: a lost case for the customer?*, 9 DIGITAL EVIDENCE AND ELECTRONIC SIGNATURE LAW REVIEW 95 – 101 (2012).

Harbison, that "Trust, by definition, is not a guarantee. Therefore an approach to understanding trust is also one of assessing risk."[33]

23. Digital technologies must be deployed in such a manner as to link persons to actions and thereby provide a necessary immutable reference for proving the authenticity of digital information over time.[34]

24. The communication of one item of software with another item of software governs much of what we do when interacting with machines controlled by software.[35]

25. Software code is subject to human technical mistakes and misperceptions of business and legal requirements. The open distributed system of communications with which we interact is very complex and subject to human design error. It is important for those involved with the law to recognize that human beings write the software that controls machines – software is the witness.[36] People make mistakes, and errors occur when writing software.[37]

26. Despite that fact that software code is subject to human technical mistakes, legal systems give presumptions of liability that renders difficult legal challenge and analysis of causation.[38]

---

[33] William S. Harbison, *Trusting in Computer Systems* 39 (University of Cambridge Computer Laboratory Technical Report No 437, December 1997) (PhD dissertation).

[34] MASON, *supra* note 27. As an example, electronic signatures and networked communications are challenged by a lack of direct evidence.

[35] Of relevance is the following observation in GEORGE DYSON, DARWIN AMONG THE MACHINES 10 – 13 (1997). ("Although our attention has been focused on the growth of computer networks as a medium for communication among human beings, beneath the surface lies a far more extensive growth in communication among machines. Everything that human beings are doing to make it easier to operate computer networks is at the same time, but for different reasons, making it easier for computer networks to operate human beings.")

[36] The untrustworthiness of evidence generated by software code and the platforms upon which it runs is examined by Sergey Bratus, Ashlyn Lembree, and Anna Shubina, in *Software on the Witness Stand: What Should It Take for Us to Trust It?*, Alessandro Acquisti, Sean W. Smith and Ahmad-Reza Sadeghi, eds, TRUST AND TRUSTWORTHY COMPUTING, LECTURE NOTES IN COMPUTER SCIENCE VOLUME 6101, 396 – 416 (Springer Berlin Heidelberg, 2010), *available at* http://www.cs.dartmouth.edu/~sergey/trusting-e-evidence.pdf; *see also* Mason and Seng, *supra* note 30, chapter 5 'Software code as the witness'.

[37] For a discussion of the imperfections of software in the context of the legal presumption that a machine controlled by software is reliable, *see* Mason and Seng, *supra* note 30, chapter 6; *see also* the general discussions in GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE 131-50 (2008):

> How to understand the workings of a complex system, such as the human brain, the climate, the economy, or an information system is one of the most difficult challenges facing modernity. It will take the law some time to develop a cogent articulation of how it should gauge the reliability of information systems. But it really has no choice but to do so."

Id. at 150.

[38] For a discussion of the undue presumption of reliability of computers and software code, see Mason *supra* note 28, at 222-4.

C. Article 29

(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.

27. Choices made by software coders that control our rights and ability to act in cyberspace reflect the goals and values of the coders and not necessarily the users. Most users do not have any knowledge of software or its biases and value choices embedded by those who write code or of how much software controls our lives.[39] When machines controlled by software fail, it is often the case that the user is blamed for the failure, rather than the relying party or service provider, which in turn has developed its own software or purchased software or software systems that are considered to be suitable for using personal information.[40]

28. All human organization requires authority. But by removing community as well as the human person as an actor with free will and choice, machines and systems controlled by software code become authoritarian and impersonal.[41]

29. The order in all systems presupposes that their components stand in specific

---

[39] For a discussion of software coders' hidden biases and value choices with respect to privacy and risk embedded in software, see Lawrence Lessig, *Code is Law*, Harvard Magazine, January-February 2000, *available at* http://harvardmagazine.com/2000/01/code-is-law-html. "The code regulates. It implements values, or not. It enables freedoms, or disables them. It protects privacy, or promotes monitoring. People choose how the code does these things. People write the code. Thus the choice is not whether people will decide how cyberspace regulates. People − coders − will. The only choice is whether we collectively will have a role in their choice − and thus in determining how these values regulate − or whether collectively we will allow the coders to select our values for us."

[40] Vining, *supra* note 14, at 25 (1986).

> In some cases, the designer of the system can be conceived as standing behind it. But it is a striking feature of machines in the modern world – particularly those to which intelligence is attributed – that they stand independent of their creators. From the time of Mary Shelley and Frankenstein the very attribution of intelligence to machines, whether or not it is correct, has resulted in this independence. Moreover, when the system is not given the attributes of intelligence and a designer can be conceived standing behind it, the designer is often not a person who cares about those the system is affecting.

[41] Authentic relations arise between persons and require a shared interactive community and common language. *See* HAROLD BERMAN (EDITED BY JOHN WITTE, JR.), LAW AND LANGUAGE: EFFECTIVE SYMBOLS OF COMMUNITY (2013) (language is a process of creating community and social relations as well as being a process of exchange, interaction, and transferring meaning.) *See also* Drucker *supra* note 21, at 260 ("For communication to be effective there has to be both information and meaning. And meaning requires communion…Communion, however, does not work well if the group is very large. It requires constant reaffirmation. It requires the ability to interpret. It requires a community.").

communicative relations to one another.[42] Therefore, in ordering both human to machine and machine to machine communications, we need shared community with a common system for configuring human rights in software code.[43]

30. We argue that if a party is encouraged to rely on software code in the machine-mediated information economy, it is imperative that a trust framework or code of conduct, such as the various United Nations model laws in the e-commerce context, provides adequately for individual autonomy, the establishment of reciprocal and enforceable rights and duties, and objectively and fairly addresses privacy risk.

31. The law must hold, and be seen to hold, the various participants in the cyber chain accountable for the systems they put in place. An effective remedy must be made available to take into account the nature of the loss. This does not necessarily mean that the usual method of assessing loss is suitable for the loss of personal information. The data protection laws in place in the European Union, for instance, generally do not provide any effective remedies to ordinary people. An organization might be subject to an administrative fine for failing to secure personal data, but the individual has little option other than to hope that their information will not be used to their disadvantage.[44]

32. Anonymity is the central characteristic of the machine-mediated information age. In this respect, an important issue is the degree of 'trust' that we can expect when interacting with a machine that is controlled by software.[45]

33. Associated with the machine-mediated information age has been a loss of both

---

[42] *See* PIERRE DE LATIL, THINKING BY MACHINE: A STUDY OF CYBERNETICS 206 – 207 (1957): "The amount of information that can be transmitted depends on a measure of the degree of order … Any signal necessarily involves differentiation. A high degree of differentiation allows all sorts of codified variations and hence a large amount of information can be carried."

[43] Dyson, *supra* note 35, at 158 – 168. *See also* Drucker, *supra* note 21, at 264 ("Indeed, the new realities with which this book deals are configurations and as such call for perception as much as for analysis…But contemporary philosophers no longer focus on Kant's concerns. They deal with configurations – with signs and symbols, with patterns, with myth, with language. They deal with perception. Thus the shift from the mechanical to the biological universe will eventually require a new philosophical synthesis.").

[44] *See* Mason, *supra* note 29, at 83 ("Failing to provide for effective and a robust means by which individuals can protect their privacy and obtain effective remedies –and the ineffectiveness of various data protection legislation across the world demonstrates the inability of governments to provide for the protection of data—means that powerful commercial interests will, in effect, become an even more significant source of influence in the future, because of the massive range of personal information they have at their disposal, regardless of how it is obtained.").

[45] Ed Gerck, *Toward Real-World Models of Trust: Reliance on Received Information* (1997), *available at* http://mcwg.org/mcg-mirror/trustdef.htm. ("Trust in cyberspace (e.g., between machines) is defined and is based on the same notion of trust, as a form of reliance, that we have been using for millennia between humans and in business.")

shared community and the capacity to make community.[46]

III. Human Rights and Digital Technologies: Emerging Recognition and Enforcement Mechanisms

34. In response, both the private and public sectors are now using Lex Informatica approaches to guide system designs and network architecture with a *human rights-oriented* paradigm.[47] Emerging programs and policies are designed to foster the configuration of software code to enable human agency, human autonomy, and subjective or claim rights.[48]

A. Configuring Human Agency

35. To provide for the ability of an individual to control access to and the use of personal data for authentication purposes, we argue that individuals need a means of digital identity that enables personal agency to act as rights-holders. The user-centric identity model is emerging as a Lex Informatica identity policy method to achieve this.[49]

36. The possibility of leveraging the blockchain to enhance informational privacy is being explored. Several organizations are promoting the concept of self-sovereign identities.[50] With this concept, the decentralized and distributed trust afforded by blockchain ledgers enables the creation of user-created and controlled digital

---

[46] Berman, *supra* note 41, at 48.

[47] Reidenberg, *supra* note 3, at 586.

> Policymakers should accept and take advantage of the distinguishing features of Lex Informatica and its usefulness for controlling information flows on global networks. Lex Informatica gives policymakers new tools to use in the development of information policy; without these new tools, information flows will marginalize national policymaking authorities. Moreover, working with Lex Informatica places policymakers at the center rather than the periphery of solutions. Lex Informatica must be seen as a distinct source of policy action. Effective channeling of Lex Informatica requires a shift in the focus of government action away from direct regulation and toward indirect influence.

[48] For an optimistic assessment, see NICHOLAS NEGROPONTE, BEING DIGITAL 228-9 (1995) ("Bits are not edible, in that sense they cannot stop hunger. Computers are not moral; they cannot resolve complex issues like the rights to life and to death. But being digital, nevertheless, does give much cause for optimism. Like a force of nature, the digital age cannot be denied or stopped. It has four very powerful qualities that will result in its ultimate triumph: decentralizing, globalizing, harmonizing, and empowering.").

[49] For a representative description of user-centric identity, see the white paper *Issues for Responsible User-Centric Identity* 2 (Center for Democracy & Technology, November 2009, Version 1.0), *available at* https://cdt.org/insight/cdt-discusses-key-policies-issues-surrounding-user-centric-identity-management/ ("This term refers to systems where users, rather than service providers, control their identity credentials.").

[50] Adam Piore, *Can Blockchain Finally give us the Digital Privacy we Deserve?* Newsweek, February 22, 2019, (describing the current rate of identity theft as an "identity crisis") *available at* https://www.newsweek.com/2019/03/08/can-blockchain-finally-give-us-digital-privacy-we-deserve-1340689.html.

identities.[51]

37. The United Nations High Commissioner for Refugees (UNHCR), in collaboration with the World Bank, has launched an effort to provide legal identities to all individuals who are stateless or lacking a birth registration.[52] To further enhance user control over digital identities and the sharing of personal information for these persons to obtain social services, the UNHCR is looking to leverage the European Union funded LIGHTest Project to enable an authoritative trust infrastructure.[53]

B. Configuring Human Autonomy

38. The User-Managed Access (UMA) access sharing protocol,[54] based on permission tokens that can be used as devices to license access rights with respect to personal digital assets collected and stored by devices, apps, and databases, provides an authoritative basis for communicating access consent as economic value. After integrating the UMA access sharing protocol, community trust can be built on legitimate and internationally recognized licenses that signal both to sending and relying parties a common understanding of legal relationships with respect to personal data. UMA permission tokens can be used as abstract contracts or credit devices for licensing informational rights in personally identifiable information, including informed consent to health information.[55]

39. Legal consent issues are especially at issue with cross-border data transfers

---

[51] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel, "A survey on essential components of a self-sovereign identity," 30 COMPUTER SCIENCE REVIEW 80-6 (November 2018) *available at* https://doi.org/10.1016/j.cosrev.2018.10.002.

[52] A description of the UNHCR digital identity programs is available at https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf. Detailed information about the World Bank's legal identity programs and goals is available at https://www.worldbank.org/content/dam/Worldbank/Governance/GGP%20ID4D%20flyer.pdf. Information on the UNHCR deployment of LIGHTest is available at https://www.unhcr.org/blogs/new-digital-solutions-refugees-education/.

[53] A description of LIGHTest Project is available at https://www.lightest.eu/ and https://www.lightest-community.org/.

[54] The UMA Version 2.0 protocol specifications can be viewed at: https://kantarainitiative.org/reports-recommendations/. UMA has been developed under the auspices of the Kantara Initiative.

[55] For a discussion of the licensing of informational rights by individuals, see Mark A. Hall, *Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records*, 95 IOWA L. REV. 631, 660 (2010) ("People should be able themselves, or through their agents, to authorize access to and use of their medical information for financial rewards, and these licenses should be transferable."). *See also*, Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125, 1134 (2000) (endorsing a licensing approach to the protection of information rights in personal data).

requirements such as the GDPR[56] and the associated sharing of personal data for identity authentication purposes.[57] A *consent receipt* is a record of a legally compliant permission provided by an individual for the sharing of that individual's personal information. Its purpose is to capture the privacy policy associated with the personal information so that the consent receipt can be easily used to communicate and manage consent and sharing of personal information once it is provided.[58]

C. Configuring Human Authority

40. Legal frameworks are now being developed that define and clarify the liability of all digital identity service providers. As an example, the Virginia digital identity law reflects public support for the creation of a market of identity service providers based on clear bases for liability.[59] By supporting a user-centric identity architecture for access to online services, the law is intended to provide Virginia citizens with a means of controlling their digital identities. The law also provides a basis for a private right of action against identity service providers for unauthorized use and transfer of personal information.

41. Related to the Virginia Identity Law as well as the eIDAS[60] in the European Union, The United Nations Commission on International Trade Law, Working Group IV, is currently preparing a draft model law for cross-border recognition of identity credentials and related trust services.[61]

42. Building on the credit union model, data cooperatives with fiduciary obligations to members provide an additional means for individuals to exercise a control over

---

[56] *See* Articles 41, 42, and 44 (1)(g) of the GDPR and Opinion 4/2017 of the European Data Protection Supervisor, sections 3.2 and 3.3. *See also* the EC Article 29 Working Party on Data Protection entitled "Guidelines on Consent under Regulation 2016/679" adopted on November 28, 2017, *available at* http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849.

[57] *See* Article 1(f)(i) of the eIDAS Regulation, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

[58] For a discussion of consent receipts, *see* the Kantara Initiative program, *available at* https://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specification.

[59] VA CODE ANN §59.1-550 *et seq*. (2015). For a discussion of legal issues involving trust frameworks in the context of identity ecosystems, see Timothy Reiniger, Jeff Nigriny, and Kyle Matthew Oliver, *The Virginia Digital Identity Law: Legal and Policy Foundations for the Identity Trust Framework Model*, ABA INFORMATION SECURITY LAW JOURNAL Volume 6, Issue 4 (Autumn 2015) at 13-26, *available at* http://www.americanbar.org/content/dam/aba/administrative/science_technology/2016/ilj_volume6_issue4.authcheckdam.pdf.

[60] The eIDAS of the European Union can be viewed at https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014.

[61] The current draft model law and related explanatory documents for UNCITRAL Working Group IV is available at https://uncitral.un.org/en/working_groups/4/electronic_commerce.

personal data.[62] A data cooperative can manage, curate and protect access to the personal data of citizen members. Furthermore, the data cooperative can run internal analytical programs in order to obtain insights regarding the well-being of its members. Armed with these insights, the data cooperative is authorized to negotiate services and discounts for its members.

43. Legal recognition for the use of video witnessing as the equivalent of personal appearance has emerged with online notarization in the United States.[63] The Law Commission of the United Kingdom has recently recommended that formal consideration be given for giving legal recognition to video witnessing as a method of satisfying a requirement for a personal appearance of a document signer.[64]

IV. Conclusion

44. This paper addresses several important legal and policy issues facing the overall challenge of recognizing and enforcing human rights in the machine-mediated age governed by software code. We contend that digital technologies must be configured by the UDHR paradigm to enable human agency, autonomy, and claim rights. Further, we contend that it is necessary in the digital age to provide for an effective and robust means by which individuals can obtain effective remedies.

45. Human agency, autonomy, and authority are three experiential realizations of digital technologies when configured in a human rights paradigm. From the legal perspective, the human rights paradigm is intended to forge information processes

---

[62] The concept of data cooperatives has been developed at the Massachusetts Institute of Technology Media Lab. For a detailed discussion, see Thomas Hardjono and Sandy Pentland, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management*, (Cornell University, May 21, 2019) *available at* https://arxiv.org/abs/1905.08819.

[63] Beginning with Virginia in 2011, twenty-two state jurisdictions in the United States have now enacted laws authorizing a remote appearance before a notary by means of audio-video communication technologies. For a detailed discussion, see Timothy Reiniger, *Developments in Information Governance, the Emergence of Online Notarization*, ABA INFORMATION LAW JOURNAL Vol. 9 Issue 4, 10-18 (Autumn 2018), *available at* https://www.asnnotary.org/files/Online%20Notarization%20%20INFORMATION_LAW_JOURNAL-volume9_issue4%202018.pdf. For a discussion of online notarization and video witnessing in the probate context, see Michael Chodos (General Counsel of Notarize) and Timothy Reiniger, *The Emergence of the Online Notary: Implications for the Probate Bar*, PROBATE & PROPERTY (A PUBLICATION OF THE REAL PROPERTY, TRUST AND ESTATE LAW SECTION, ABA), Vol. 33, No. 4, 59-62 (July/August 2019).

[64] Law Commission, *Electronic execution of documents* 111 (Law Com No 386, HC26240, 2019) (sections 7.6 and7.7), *available at* https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2019/09/Electronic-Execution-Report.pdf. (The Law Commission is the statutory independent body created by the Law Commissions Act 1965 to keep the law of England and Wales under review and to recommend reform where it is needed.)

that are authoritative and prevent the authoritarian.[65]

Timothy Reiniger is an attorney specializing in information law and policy (licensed to practice in California, the District of Columbia, and Maine). He has served as an ABA-appointed advisor to the Uniform Law Commission and is an author of both the Virginia online notarization law (2011) and the Virginia digital identity law (2015). As a former Executive Director of the National Notary Association, he is recognized as an expert in notarial law, providing testimony on this subject before the United States Congress and over twenty state legislatures. Currently, he serves on the advisory board of the EU's LIGHTest Project (Horizon 2020) and is Director of the Reiniger LLC in Cape Elizabeth, Maine. He can be reached at tim@reinigerllc.com.

Stephen Mason is barrister. He was invited by the Law Commission to be a member of the Advisory Panel of experts for the report entitled *Electronic execution of documents*. Stephen the author of the open source practitioner text *Electronic Signatures in Law* (4th edn, 2016), and the co-editor, with Daniel Seng, of the open source practitioner text *Electronic Evidence* (4th edn, 2017), and the editor of *International Electronic Evidence* (2008). He is the founder of the international open source journal *Digital Evidence and Electronic Signature Law Review*. He can be reached at stephenmason@stephenmason.co.uk.

---

[65] The authors praise the United Nations for seeking to extend human rights principles to the digital technologies. The UDHR, like the lighthouse that provides safety to vessels, serves as a beacon providing safety to human beings in the machine-mediated age government by software code. Accordingly, we find the following passage as an apt close to this submission:

> "Sail on!" it says, "sail on, ye stately ships!
> And with your floating bridge the ocean span;
> Be mine to guard this light from all eclipse,
> Be yours to bring man nearer unto man!"
> -- Henry Wadsworth Longfellow (*The Lighthouse*, 1849)