



# Five Freedoms for the *Homo Deus*

**Omer Tene** | International Association of Privacy Professionals

**Jules Polonetsky** | Future of Privacy Forum

**Ahmad-Reza Sadeghi** | Technische Universität Darmstadt

In his book *Homo Deus: A Brief History of Tomorrow*,<sup>1</sup> Yuval Noah Harari evokes the specter of humanity ruled by an all-knowing, omnipresent data processing system. He envisages that “Dataism,” a universal faith in the power of algorithms, will become sacrosanct, with increasingly irrefutable automated decisions subjecting humanity to the tyranny of an algorithmic overlord. He projects that the forces of technology and globalization will herald the demise of the very liberal freedoms that enabled them.

In this special issue of *IEEE Security & Privacy*, researchers from across disciplines discuss strategies to prevent the realization of this bleak vision, in which artificial intelligence (AI) defeats liberal values, including privacy, equal protection under the law, and due process. Based on their work, we propose five freedoms for the *Homo Deus*, legal and ethical guidelines to overcome the risks of a soulless digital age: freedom from secret agendas, freedom to access data for good, freedom from censorship, freedom to understand the logic of the machine, and freedom to stay human. We explain each proposed principle below.

## Freedom from Secret Agendas

In “Taming the Golem: Challenges of Ethical Algorithmic Decision Making,”<sup>2</sup> we proposed requiring platforms to make clear whether their services are driven by “neutral” algorithms or by systems that proactively editorialize. While even policy-neutral algorithms reflect existing societal biases and historical inequities, policy-directed algorithms are purposely engineered to advance a predefined normative agenda. Individuals should know whether content they view, smart home sensors they operate, devices they wear, and apps they download operate on their behalf or to further a corporate or government policy. Several authors in this issue, including Robert H. Sloan and Richard Warner, in their article, “When Is an Algorithm Transparent?: Predictive Analytics, Privacy, and Public Policy,” stress the importance of transparency obligations for organizations that employ an active, digital editorial hand.

## Freedom to Access Data for Good

The growing concentration of data in the hands of a few platforms will not be solved by simply hemming in large companies. As long as organizations retain the right to do business, network effects will empower certain businesses with access to more data and better tools of analysis than those available to the public at large. Inevitably, governments and companies will grow smarter about individuals' lives, health, movements, and behaviors. Society's challenge will be to ensure that the secret magic of big data does not remain the domain of only a select few, fulfilling Harari's grim prediction of digital haves and have-nots. Currently, concerns over ethical restrictions and legal impediments, including privacy and data protection laws, threaten to diminish society's use of data for good. For example, provisions in Europe's General Data Protection Regulation (GDPR) requiring data minimization and purpose specification jeopardize productive collaboration between researchers and private sector businesses. In "Privacy Protective Research: Facilitating Ethically Responsible Access to Administrative Data,"<sup>3</sup> we suggested privacy-protective strategies for enabling productive use of data about populations without risking exposure of or knowledge about any specific individuals. In this issue, Bernd Carsten Stahl and David Wright, in "Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation," as well as Micah Altman, Alexandra Wood, and Effy Vayena in "A Harm-Reduction Framework for Algorithmic Fairness," suggest strategies for facilitating researchers' ethical access to data.

## Freedom from Censorship

In some countries, policy initiatives to limit access to platforms and edit online content are neither new nor theoretical. The activities of Chinese companies that proactively scan for content that government officials find offensive once seemed Orwellian. But even in Western democracies, the vitriol of today's messy online world has prompted some prominent scholars to call for scaling back freedom of speech and support new penalties on platforms for user-generated content. Germany, for example, has just passed legislation penalizing companies for offensive content, and even in the US, the bulwark of Section 230 immunity from intermediary liability is beginning to crack. Would restricting online speech or imposing new obligations on digital platforms effectively reduce fake news, hate, and incitement? In a complex normative environment, crude policy solutions can backfire. Imposing weighty legal and social responsibility on digital platforms also means assigning them with great decision-making power. In its right to be forgotten decision, the European Court of Justice seated Google as an ultimate arbiter of what personal

information is "adequate, relevant and not excessive."<sup>4</sup> In the fake news context, appointing online platforms as "ministries of truth" to decide what content is desirable and steer users to appropriate channels would be both futile and undemocratic. This does not mean we are doomed to live with hate-filled online discourse. But blaming technology for the difficult state of our politics and public debate is far easier than addressing real deep-rooted challenges. Legislating requirements for tech companies to actively police digital content is simpler than taking a hard look at what is failing in our education system, electoral process, government, religious and civic organizations, and community life. If these institutions are in crisis, focusing our efforts on technology may treat just the symptoms while ignoring their cause.

## Freedom to Understand the Logic of the Machine

In "Big Data for All: Privacy and User Control in the Age of Analytics,"<sup>5</sup> we suggested, first, that organizations should provide individuals with practical, easy-to-use access to their information in machine-readable format, so they can become productive participants in the data economy. Second, we recommended that organizations be transparent about the decisional criteria underlying their data processing activities, allowing individuals to challenge, or at the very least understand, how decisions about them are made. This does not mean sharing indecipherable—and secret—algorithms, but rather, much like consumer reporting agencies do in the context of the Fair Credit Reporting Act, revealing the decisional criteria used in automated decision-making processes. In "Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'?", Lilian Edwards and Michael Veale recommend a slate of legal and paralegal remedies to impel the creation of better and more scrutable algorithmic systems.

## Freedom to Stay Human

As Danielle Citron explained in "Technological Due Process,"<sup>6</sup> automated systems jeopardize due process norms. A new concept of technological due process is essential to vindicate the norms underlying traditional procedural protections. In its provisions on automated decision making, for example, the GDPR requires organizations to keep human reviewers in the loop. An independent human decision maker, such as a European Data Protection Officer (DPO), is a step in the right direction. In "Beyond IRBs: Ethical Guidelines for Data Research,"<sup>7</sup> we proposed the creation of new corporate institutional review board (IRB) constructs to vet new data projects and provide individuals with due process and recourse. In their piece, "Proactively Protecting

Against the Singularity: Ethical Decision Making in AI,” Dawn E. Schrader and Dipayan Ghosh emphasize the importance of human actors softening the blunt edges of Harari’s impending data machine. In “AI and the Ethics of Automating Consent,” Meg Leta Jones, Ellen Kaufman, and Elizabeth Edenberg propose harnessing AI tools to increase individual agency and choice.

**W**ith evidence mounting about the proliferation of “fake news” and hate speech online, policymakers around the world are already struggling to address the impact of new technologies on elections and public discourse in democratic societies. Digital platforms, once seen as a force for good and a driver for economic prosperity, dissemination of knowledge, and broad social participation, are now accused of becoming a vehicle for disinformation, discrimination, and injustice. In his piece, “What Can Political Philosophy Teach Us about Algorithmic Fairness?,” Reuben Binns places such highly charged terms, as well as notions of algorithmic fairness and egalitarianism, into a broader philosophical context. Yet, while the regulatory instinct may be to rein in AI, algorithms, and digital platforms, we should be cautious of knee-jerk reactions to complex public policy dilemmas. In a world where data and technology are increasingly the purview of a few leading companies and governments strive to set the rules of the Internet to better control populations and commerce, how can we ensure that individuals continue to have agency over important decisions affecting their lives? ■

## References

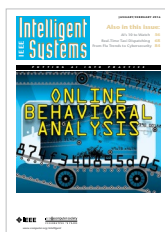
1. Y.N. Harari, *Homo Deus: A Brief History of Tomorrow*, Harper, 2017.
2. O. Tene and J. Polonetsky, “Taming the Golem: Challenges of Ethical Algorithmic Decision Making,” *North Carolina J. Law and Technology*, vol. 19, 2017.
3. D. Goroff, J. Polonetsky, and O. Tene, “Privacy Protective Research: Facilitating Ethically Responsible Access to Administrative Data,” *Annals of the American Acad. Political and Social Science*, 675, Jan. 2018.
4. *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez*, Case C-131/12, 2014 E.C.R. 317, par. 89–99, 13 May 2014; [http://curia.europa.eu/juris/document/document\\_print.jsf?doclang=EN&docid=152065](http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065).
5. O. Tene and J. Polonetsky, “Big Data for All: Privacy and User Control in the Age of Analytics,” *Northwestern J. Technology and Intellectual Property*, vol. 11, no. 5, 2013.
6. D.K. Citron, “Technological Due Process,” *Washington Univ. Law R.*, vol. 85, no. 6, 2008.
7. O. Tene and J. Polonetsky, “Beyond IRBs: Ethical Guidelines for Data Research,” *Washington and Lee Law R. Online*, vol. 72, no. 3, 2016.

**Omer Tene** is vice president and chief knowledge officer at the International Association of Privacy Professionals. Contact at [otene@iapp.org](mailto:otene@iapp.org).

**Jules Polonetsky** is CEO of the Future of Privacy Forum. Contact at [julespol@fpf.org](mailto:julespol@fpf.org).

**Ahmad-Reza Sadeghi** is a professor of computer science at Technische Universität Darmstadt. Contact at [ahmad.sadeghi@trust.tu-darmstadt.de](mailto:ahmad.sadeghi@trust.tu-darmstadt.de).

# stay on the Cutting Edge of Artificial Intelligence



**IEEE Intelligent Systems** provides peer-reviewed, cutting-edge articles on the theory and applications of systems that perceive, reason, learn, and act intelligently.

