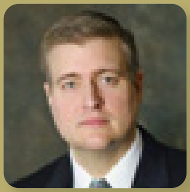
PRINCIPLES OF DIGITAL LAW AND ETHICS



BY
THOMAS FREEMAN

&
DR. AARON MCKAIN

Thomas J. Freeman, JD, MS, MBA, is a Business Law Professor at Creighton University, a practicing attorney, and the Director of Research and Policy Analysis at the Institute for Digital Humanity. Aaron McKain, Ph.D., M.S.L. is the Director of the School of English and Communication Arts and Associate Professor of Digital Media at North Central University, as well as the Executive Director of the Institute for Digital Humanity. The authors would like to thank: Samson Hall is a Research Associate for the Institute for Digital Humanity. Joseph Masi, Michael Bartz, William Harper, Kylie Karsky, Madeleine Britto, C.J. Braccia, Emily Atamov, Ava Verzani, and Clare Hart are students at Creighton University and contributed to this article.

TechREG CHRONICLE
FEBRUARY 2023

Visit www.competitionpolicyinternational.com
for access to these articles and more!

PRINCIPLES OF DIGITAL LAW AND ETHICS

By Thomas Freeman & Dr. Aaron McKain

As more personal data is collected and more decisions that affect individuals are automated, individual rights are increasingly threatened. The legal system and society at large need to determine what information about individuals can be gathered and maintained and when and how that data can be used to judge individuals. It is essential that we have thoughtful conversations about the core principles for digital law and ethics. Those conversations should involve broad, diverse, and interdisciplinary groups, which can consider factors such as biases in historical data, whether an algorithm is being programmed or trained appropriately, and what type of decisions we are comfortable automating or trusting algorithms to make. The best safeguard of our digital rights will ultimately be engaging diverse teams that thoughtfully consider how their fellow humans are affected as they establish legal and ethical guardrails around emerging technology.

We live in an era of Big Data, where most information about us is known or knowable. Gone are the days when privacy consisted of the ability to choose what we shared with the world. We spend more and more of our lives online. Our online activities, movements, purchases, and communications are tracked, cataloged, and used to judge and influence us. There are almost no rules for this Brave New World we live in, which permits our government(s) and private companies to engage in all manner of questionable practices that would have been unthinkable – violating state and federal law as well as industry and civic norms – only a decade ago.

If we do not change course quickly, hard-won privacy and civil rights can be lost, possibly forever. There is a desperate need for legal regulation and ethical guardrails for the digital world. An emerging industry is sprouting up to fix the messes caused by corporations and governments vacuuming and monetizing personal data. However, there is a conspicuous lack of careful attention to some basic and fundamental questions of digital ethics and law. What types of information about people should be allowed to be gathered about patients, students, defendants, and citizens? How should the governments and corporations that gather it be allowed to use it? When and how should data about individuals be used to make decisions about them that affect their abilities to secure housing, medical care, employment, parole, or probation? When algorithms or other automated processes are designed to make decisions about people, what safeguards are necessary to ensure those decisions are accurate and free from bias?

Digital ethics doesn't pertain to one piece of technology or another. It's an ecosystem that demands a public referendum on what personal information should be private, how automated decisions should be made, what information should be censored (and by whom), and what it means to be a citizen or person in criminal, employment, educational, financial and health care contexts. Programmers, policymakers, teachers, advocates, and lawyers struggle to adequately address these issues. Legislators and courts are asking for help because they cannot keep up with rapidly evolving technology. The digital ethics community has few proven holistic solutions accepted across industries, education levels, and academic disciplines. There is a danger that ideological divisions could become entrenched and block effective bipartisan coalitions and solutions.

As a guide to addressing these concerns, this article will attempt to lay out the core principles for digital law and ethics, gleaned from both the author team's research and their experience with their technology ethics initiative: The Institute for Digital Humanity. Started in 2018, the IDH is a bipartisan and multi-faith digital rights think tank that works to secure the rights of everyone. And by following some basic principles of digital ethics and constitutional law, the IDH has found a "cheat code" that should be of interest to any organization that is serious about reclaiming civil rights. We begin this article by outlining some overarching principles of digital ethics and constitutional law. Then we turn to two specific examples – privacy and algorithmic decision-making – to show how these principles apply.

01
DIGITAL LAW AND ETHICS

Although it seems overwhelming, the issues regarding how to regulate this new digital world can be distilled into two fundamental questions: 1) what information about us can be gathered and retained, and 2) how can it be used to judge us? With those guidelines in mind, we have developed a list of core digital rights principles.

A. Core Principle #1: Digital Ethics and Law Issues Require a Holistic Approach

Privacy and AI decision-making are often the central focus of AI ethics reform. But *all* digital ethics issues must be dealt with holistically and based on consistent principles. While the case studies in this article deal explicitly with AI decision-making and intrusions into privacy that would have been unethical or illegal in the pre-digital age, these methodologies and principles have been developed – and are compatible with – the two other and irretrievably interconnected, primary digital threats to our civil rights and democratic values:

- *Disinformation/Misinformation:* Who decides what information misleads or is false and should be censored as a result? What rules or guidelines should be used to make those determinations? All of us are uncomfortable with the fake news and conspiracy theories we see online. But who do we trust to identify those and determine whether we should be allowed to view them and judge them for ourselves?

- What are the rules of behavioral advertising and political micro-targeting?

- *Rebalancing Free Speech Versus Hate Speech: How can we determine when to suppress online speech? When does speech become so hateful that it must be censored? Who should be empowered to make those decisions? What standards should be used for making those decisions?*

B. Core Principle #2: Give Everyone a Seat at the Table: Digital DEI

Digital ethics affects all of us. This is an enormous and diverse world. Every person in it has a stake in how key digital civil rights issues – from privacy to algorithmic discrimination to disinformation to free speech versus online hate speech – are determined. Every political, cultural, or religious faction can veto any tech solution. The teams composed to design, assess, and evaluate algorithms must be truly diverse, based on the presence of those with different races, genders, ages, disability statuses, etc., as well as of thought leaders from various industries, professions, academic fields, backgrounds, and worldviews. A trusted leader from a particular minority community can explain how members of that community might be affected by or react to a product or service. Historians, philosophers, attorneys, and industry leaders can bring unique insights about how a data set is biased or a practice might be illegal or impracticable. If humans are to be weighed, measured, and judged by algorithms, those algorithms should at least be intelligently and thoughtfully designed.

C. Core Principle #3: Interdisciplinary and Peer-Reviewed Methods

Digital ethics, by its nature, is an interdisciplinary field. The practices of effectively designing and evaluating digital tools and policies will require diverse groups of people drawn from different industries and academic fields. Lawyers, ethicists, philosophers, historians, writers, and artists must be included in those conversations, as they can all bring different perspectives. The methods by which they assess questions like what types of data collection should be permitted or when an algorithm should be allowed to judge a person should be peer-reviewed to ensure they work as intended. Too many unintended problems caused by unregulated technology occurred because the experts from various disciplines, and with diverse life experiences were not consulted before implementation. It would help if you had a methodology — and here, the IDH uses narrative theory, but there are others – that are accepted and valued (and considered unbiased) by multiple professional and academic communities.

D. Core Principle #4: Teachable and Understandable to Everyone

Our lives are increasingly lived online. Our resumes are stored on sites like LinkedIn. Our thoughts are collected on applications like Facebook, Instagram, and TikTok. Algorithms are increasingly making decisions about us. These systems of data collection are almost inescapable. Each interaction with the world is increasingly monitored, cataloged, and used for algorithmic assessment and/or prediction. It is, therefore, vital that individuals understand how and why they are being judged. And principles of digital ethics – while complex enough to be of use to lawyers, legislators, policymakers, and programmers – need to be simple enough that anyone can understand them to both know and express their rights.

02

RETHINKING THE RIGHT TO PRIVACY

How the world views us is increasingly a function of how we conduct ourselves online. We view news stories, advertisements, and other online content based on who tech companies think we are. How do you carve out a "private" space for your identity when "how" you present yourself (via social media, search engines, browser clicks, and purchases) is radically re-contextualized and algorithmically calculated by – to name just a few prominent examples – future schools, employers, retail companies, political advertisers, and police departments? The state of U.S. privacy law remains in flux, with states such as California trying to go it alone with laws like the California Consumer Privacy Act ("CCPA"). To date, the United States has yet to pass any comprehensive laws regarding privacy similar to Europe's General Data Protection Regulation ("GDPR").

There is a common misconception – regrettably shared even within the digital ethics community – that privacy no longer exists. This is both dangerous and patently incorrect in the context of post-digital Constitutional law in the United States. The right to privacy still exists, but in the era of Big Data needs to be reconceptualized: It isn't the right to privacy that has disappeared. It's the traditional view of *privacy as secrecy* that no longer works. As Justice Alito argued in *U.S. v. Jones*, if "an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," and almost all information about us is known or discernible in the post-digital era, then privacy, as a legally protected concept, would, wrongly, cease to meaningfully exist. ("I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[2]

More importantly, Alito recognizes that the nature of privacy as a protected Constitutional right turns on – both philosophically and legally – what the public "believes" its rights to post-digital privacy are, both affirmatively and via the traditional violations of privacy that they are – every day in the post-digital era – acquiescing to. Every judgment we make – whether to use that CVS card on our keychain or to turn on our GPS – is unavoidably larger than itself and an *epideictic* declaration of our values.

The modern right to privacy will need to shift from a singular focus on "what is shared" – by acknowledging the reality that most information about us has already been collected or can be ascertained based on statistical guesswork – to a

[2] *U.S. v. Jones*, 565 U.S. __ (2012), slip op., Sotomayor concurrence at 5.

symbiotic legal/cultural paradigm that asks “whether, when, and how” information about us can be used to form judgments and make decisions about and against an individual: How was the information about the individual obtained? How old was the person at the time of the alleged misdeed? What were the circumstances surrounding it? As we are increasingly deprived of the ability to maintain secrets or personal information, we must become more thoughtful and intentional about how people are judged and when they should be forgiven. Even after perhaps the most shunning in literary history, Hester Prynne earned back her community's respect.[3] The modern world will likewise have to think about the concept of forgiveness.

> *There is a common misconception – regrettably shared even within the digital ethics community – that privacy no longer exists*

The erosion of privacy has been a slow-moving crisis for decades. A more holistic approach to privacy is needed, which envisions it as an ecosystem of public, private, and professional decisions about when, where, and why data should be, legally and ethically, allowed to be used as evidence when making judgments and interpretations about particular people in particular contexts.

A. Privacy Value #1: Transparency and Knowing Consent

The targets of any data collection should have to consent to it. That consent must be premised on full and fair disclosure about the data collection. Knowing consent requires that those who collect our data disclose what they are gathering and doing with it. Those whose data is collected should have the right to withdraw their consent and request that their data not be used in a certain way or deleted entirely.

B. Privacy Value #2: Evidence Exclusion Rules

When do we allow data about someone to be used as evidence against them? In a criminal context, evidence that is the product of an unreasonable search or seizure cannot be used against a defendant. But this principle – an “evidence exclusion rule” – is also a key means to methodologies of a critical privacy value in all data contexts (financial, medical, educational, etc.): *Interpretive restraint*. Or, to put it in less legal terms: “Evidence exclusion” means a determination that, despite the known availability of potential interpretive evidence (which, in the digital era, includes everything from emails to social media posts to search engine histories), an organization, government agency, or community has chosen (for ethical, practical, legal, and/or political reasons) to exclude and ignore this data when making a judgment, analysis, or prediction about this particular person or group of people.

C. Privacy Value #3: Forgiveness and Grace:

The notion of a statute of limitations on shunning, shaming, or cancellation should also be explored. In our view, we must create a clear and unifying version of the right to be forgotten in the United States and perhaps the world.[4] We have all read stories about someone making a poor decision or social media gaffe. In one recent example, an 18-year-old cheerleader was “canceled” and forced to withdraw from college due to her unfortunate use of a racial epithet years before when she was 15 years old. For the rest of her life, anytime anyone performs a web search for her name, the first page of search results will recount a dumb and embarrassing thing she did as a child.

Forgiveness and grace need to be a cornerstone of our social ethos. As previously discussed, our collective data is out there and is there to stay. We have seen the effects of cancellation already, but as more of us live more of our lives online, our society will face this problem on a much larger scale.

Generation Z is the first generation to have social media as a part of their whole lives. Social media companies alike have been tracking, collecting, and utilizing personalized data they started collecting from users when they were children. These individuals are now applying for colleges and jobs and entering adulthood. This means the call for forgiveness and grace must be even stronger. We have a generation who has spent much of their lives on social media without a second thought. The information they shared, even casually and thoughtlessly, can come back to haunt. As a society, we must ask ourselves if we want to shun, shame, and/or cancel individuals when they might have changed, but their data has followed them forever.

As a society, we must build a collective post-digital ethos around privacy. These new standards and community norms must include such quaint but critical notions as understanding, forgiveness, and grace. That should start with some form of right to be forgotten, where an individual can ask search engines to delete stories about their past, so long as they do not concern criminal behavior or a matter of ongoing public interest.

[3] Hawthorne, N. (1850). The Scarlet Letter. Boston, MA: Ticknor and Fields.

[4] Everything you need to know about the “Right to be forgotten,” GDPR-EU, https://gdpr.eu/right-to-be-forgotten/?cn-reloaded=1.

03

RE-PROGRAMMING AND REFORMING ALGORITHMIC DECISION MAKING

An increasing number of the decisions once made by humans are now made by algorithms, which are automated processes used by computers. Algorithms are also increasingly used by prospective employers, landlords, businesses, health providers, police, schools, and government agencies to determine whether individuals are worthy of jobs, housing, health care, education, parole, or probation. The laws we have put in place to guarantee civil rights are premised on human actors making decisions that affect people. In post-digital America, regulations and Constitutional precedent are still in the early stages of determining how to enforce civil rights laws on computer processes.

People too often treat algorithms like calculators and their decisions like solutions to math problems. Algorithms are step-by-step sequences of instructions we direct computers to use. When a machine is tasked with something objective, like adding two numbers, we can reliably trust and use the answers it produces. However, in the post-digital world, machines are often tasked with complex decision-making that cannot be reduced to binary code (i.e. algorithmic error rates); they fail to understand the "intersectional" nature of our fellow citizen's identities (i.e. algorithmic discrimination); unjustly use prior data to re-reinforce old stereotypes and systemic disadvantages; or fail to holistically judge and evaluate an individual and their circumstances (as employees, defendants, patients, and suspects).

While numerous organizations and influencers now provide "solutions" to algorithmic decision-making – including the White House's AI Bill of Rights – these solutions often simply "re-program" the ideological divisions already blocking meaningful reform. More troubling, by focusing narrowly on particular types of discrimination (i.e. Race and gender), current "solutions" further marginalize other protected categories of identity. Even worse, they inadvertently program in a "separate but equal" digital society that legal scholar Margaret Hu has rightfully called "Algorithmic Jim Crow."

We utilize the following core methodological principles as a bipartisan and interdisciplinary solution that works with any AI decision-making process.

A. AI Decision-Making Principle #1: Transparency and Consent

Those who use algorithms to make decisions should be required to notify those affected by those decisions that 1) algorithms are judging them and 2) how those algorithmic judgments are rendered. Transparency and consent also trigger these sub-concerns, values, and questions about data sets, machine learning, and burden shifting.

- ***Data Sets****:* What data sets are used to train algorithms? Are they trained on large, diverse, and representative data sets? Have those datasets been evaluated thoughtfully and measured for historical biases? Are they regularly audited to ensure they are making decisions fairly and in a manner free from bias? Do the parties using them understand why and how they make decisions? Can their decisions be explained and replicated? When technology is not designed with thoughtfulness and intentionality about how it can affect different groups of people, the results can be disastrous.

- ***Machine Learning****:* The processes of how an algorithm is designed and learns, what techniques it uses for training and validation, how it makes decisions, how it is audited and evaluated, and whether it is working as intended must be fully transparent and explainable. Those affected by its findings, the legal community at large, government regulators, etc., must be able to "see" and understand how and why the algorithm makes decisions so those decisions can be evaluated for legality and fairness.

- ***Burden Shifting****:* Our legal system is designed to evaluate how humans make decisions regarding other humans. The individual who believes an algorithm judged them unfairly should not have to bear the burden of proof, which could be quite costly. Instead, the parties using algorithms to evaluate individuals and determine their qualifications should be forced to explain how the algorithms work and unpack and justify their decisions. For example, suppose an algorithm is used during job interviews for a position and prefers one candidate over another. In that case, the company using the algorithm must have an affirmative duty to explain how it works and why it formed that opinion.

Once these transparency questions are answered, digital ethics and law demand a more holistic approach to how AI renders decisions. This brings us to three more principles for meaningful AI reform: Error rates, bias and discrimination, and human oversight when technology is making life-altering decisions about people.

B. AI Decision-Making Principle #2: Error Rates

A quick sampling of recent algorithmic injustice instances highlights this growing problem. In terms of algorithmic error rates, Bank of America was recently fined 225 million dollars and ordered to offer redress, which could amount to millions more for a fraud detection algorithm that lacked human oversight.[5] Predictive policing algorithms are proving to be inherently flawed and rely on historical crime data which replicate discriminatory police practices and reinforces over-policing of communities of color and is not guaranteed to predict a crime.[6] Individuals like Robert McDaniels found themselves on the Chicago Police Department heat list [even with no history of violence]. McDaniels became the subject of police harassment and constant surveillance, which led to him being shot twice.[7]

> *A quick sampling of recent algorithmic injustice instances highlights this growing problem*

C. AI Decision-Making Principle #3: Bias and Discrimination

A key reason algorithms exhibit error rates, and biases is that they are trained on flawed datasets. Algorithms are asked to predict the future based on the past. It should be no surprise that many racial, gender, and other biases are built into historical datasets. These biased datasets are also called coding bias and, if left uncorrected, reinforce decades of marginalization and discrimination.

The U.S. Department of Justice recently settled a case against Meta Platforms (formerly Facebook) for allowing features in its advertising business to discriminate against groups protected by federal civil rights laws.[8] The Correctional Offender Management Profiling for Alternative Sanctions ("COMPAS") algorithm predicts the likelihood of a criminal defendant's recidivism.[9] COMPAS predicted twice as many false positives for recidivism for black offenders (45 percent) than for white offenders (23 percent). Facial recognition programs are used to make employment decisions and identify criminal suspects, despite often struggling to "see" darker skin.[10] Algorithms used to find more "high quality" or "successful" job candidates can look for "more of the same," replicating a company's biased historical hiring practices and overlooking qualified candidates who belong to historically marginalized groups.[11]

In situations with a higher-than-normal risk that an algorithmic assessment might be incorrect and/or biased, consideration should be given to restricting the use of algorithms and insisting on human decision makers. For example, a facial recognition program that judges a person's personality based on their facial expressions might judge someone who is non-neurotypical harshly. In such cases, human assessors who can consider such factors would likely be more appropriate.

D. AI Decision-Making Principle #4: Human Oversight When Machines Judge People

In our view, algorithmic decision-making has yet to advance to the level where it should be completely autonomous and unaccountable. The explosion of systems that determine everything from who gets a job to who gains access to housing or medical care or is granted parole or probation is very concerning. Algorithms offer us increased convenience and efficiency: They can enable companies to review massive amounts of data far more quickly than humans could. But we should ask ourselves, should we ever allow a machine, no matter how alike in human consciousness, to be able to be free of human oversight? It is imperative that diverse groups of humans, with careful deliberations, thoughtfulness, and intentionality, ensure that algorithmic judgments are made correctly, in a manner free from bias, and with due respect to privacy when life-changing decisions – economic, medical, educational, legal, professional, and/or financial – about our fellow humans are at stake.

[5] Jenna McNamee, CFPB fines Bank of America for faulty unemployment benefits fraud detection, Jul 18, 2022, https://www.insiderintelligence.com/content/cfpb-bank-of-america-faulty-fraud-detection.

[6] Pitfalls of Predictive Policing: An Ethical Analysis Viterbi Conversations in Ethics Volume 6 Issue 1 17 February 2022; see also Predictive Policing Explained Brennen Center for Justice, Tim Lau, 1 April 2020.

[7] Heat Listed - Chicago PD automated Policing Got a Man Shot Twice , The Verge - Matt Stroud, 24 May 2021

[8] Jenna McNamee, CFPB fines Bank of America for faulty unemployment benefit fraud detection, Jul 18, 2022, https://www.insiderintelligence.com/content/cfpb-bank-of-america-faulty-fraud-detection.

[9] Terence Shin, Real-life Examples of Discriminating Artificial Intelligence, Towards Data Science, Jun 4, 2020, https://towardsdatascience.com/real-life-examples-of-discriminating-artificial-intelligence-cae395a90070.

[10] Reuters, Thomas, Black and Asian faces misidentified more often by facial recognition software, Dec 20, 2019, https://www.cbc.ca/news/science/facial-recognition-race-1.5403899.

[11] Bogen, Miranda, All the Ways Hiring Algorithms Can Introduce Bias, May 6, 2019, https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias.

04

CONCLUSION

The era of Big Data requires a rethinking of legal and ethical principles. If we are to have a right to privacy, the parameters of it must be based on how data can be used. If we are to be judged by machines, the algorithms that make them and the judgments they make will need to be carefully monitored. And the best safeguard of our digital rights will ultimately be engaging diverse teams that thoughtfully consider how their fellow humans are affected as they establish guardrails around emerging technology. ■

> *This article highlights only a few of the ways that blockchain networks and Web3 applications may open new ways to approach antitrust analysis for zero-price goods*