

A Primer on Digital and Data Science Ethics

by Thomas Freeman, Aaron McKain, and Samson Hall
with Joseph Masi, Matthew Mandolfo, Madeleine Britto, Michael Bartz,
William Harper, Kylie Karsky, Meagan Compton,
Emily Atamov, the Creighton Business Law Research Forum,
and the Institute for Digital Humanity¹

As the pace of technological change accelerates, the law is struggling to catch up. What happens to individual privacy in a world where so much data has been collected that our ‘secrets’ are mostly known? Who will be held responsible for civil rights violations committed by machines? How must our courts adapt when more and more lawsuits will challenge these algorithmic decisions?

These are the questions this author team has been confronting on a daily basis as the leaders, employees, and interns at the Institute for Digital Humanity (IDH), a non-partisan, student-run digital ethics think tank based in downtown Minneapolis. Born at North Central University—a Christian college that gained international fame as the host site of the George Floyd Memorial—the IDH has, in four short years, done the politically impossible: bringing together a diverse and cross-cultural coalition of academics, advocates, lawyers, and educators to fight together for a just, sane, and equitable post-digital world. Using our proven and peer-reviewed methodologies—to teach, consult, and program the legal complexities of privacy, algo-

rithmic discrimination, and disinformation—the IDH and its partners (including the ACLU, Anti-Defamation League, Civic Nebraska, Indiana University, and the Netflix *Coded Bias* documentary team)—have launched successful K-12 and undergraduate curricula, aided in the successful banning of racist facial recognition technology in Minneapolis, and are currently working with the ADL, the ACLU, and a variety of other partners on projects related to digital and data science ethics.²

What is striking to us, however, is how many members of the legal community still lack a foundational understanding of the legal dangers and constitutional questions of our post-



Thomas Freeman



Thomas Freeman (JD, MS, MBA) is a Business Law and Ethics Professor at Creighton University, practicing attorney, Senior Researcher and Policy Analyst at the Institute for Digital Humanity, and Director of the Creighton Business Law Research Forum.

Aaron McKain



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, a student-run digital ethics think tank in downtown Minneapolis. His publications and public appearances on digital ethics, politics, and law can be found at aaronmckain.com.

Samson Hall

Samson Hall is a current Research Associate at the Institute for Digital Humanity, a student-run digital ethics think-tank in downtown Minneapolis, having worked on a variety of IDH projects including curriculum creation, grant writing, op-eds, and academic works.

A PRIMER ON DIGITAL AND DATA SCIENCE ETHICS

digital moment. For the uninitiated, this article—written with our 2022 summer interns at Creighton University—serves as a primer on algorithmic bias and misuse, and as an invitation, as always, to partner with the IDH to fight for the civil rights of all citizens during this critical technological sea change.

Rethinking Privacy in the Era of Big Data

In 1890, Samuel D. Warren and Louis D. Brandeis presented a compelling case for a right to privacy, providing a short-hand definition of the concept as the “right to be let alone.”³ In the view of Warren and Brandeis, this right revolved around an individual’s choice to determine which parts of themselves were shared with the world through publication or other communication. In the post-digital society we currently reside in, such a notion has become increasingly quaint. Pandora cannot be put back in the box, and individuals are permitted very few, if any, secrets. Companies and governments—hypothetically and often literally—track our every digital purchase, search, social media post, phone call, email, and text message. Even when a phone or mobile device is not being used, the device and its applications are often still tracking our movements and locations.⁴ The rate of data collection, along with data storage potential, continually grows at an exponential rate. Even more concerning, these records can be stored and potentially used against a citizen’s interests indefinitely.⁵

This is, of course, a privacy crisis of unparalleled proportions. And, as the Supreme Court has noted—most notably in *U.S. v. Jones*—until our citizens begin to assert what we believe our new rights, duties, and obligations are in an era where we have access to some much previously private and personal information, our Constitutional and legal safeguards are in jeopardy. The U.S. Supreme Court has held that when weighing the Constitutional guarantee of a “reasonable expectation of privacy,” a judge’s decision can no longer rest upon:

the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.⁶

So what does this mean, practically, in terms of privacy and our legal rights? To better understand these magnitudes and risks, let’s quickly turn to a particular area of IDH research: student data privacy.



68th Annual

Federal and State Income Tax Institute

In-depth updates in federal and state tax law and regulations that fulfill CE credits for attorneys, CPA, IRS, EA, CFP and other legal professions.

REGISTER NOW ► TAXINSTITUTE.UNL.EDU

More Professional Development Options

Executive and professional development that addresses rapidly changing business needs ► **BUSINESS.UNL.EDU/EXECED**

ATTEND IN PERSON OR ONLINE

Scottsbluff: Nov. 7-8

Kearney: Nov. 10-11

Grand Island: Nov. 14-15

Omaha: Nov. 28-29

Norfolk: Dec. 1-2

Lincoln: Dec. 5-6

Livestream Dates:

Nov. 17-18

Nov. 28-29

Dec. 5-6



**IRS-APPROVED
CONTINUING EDUCATION
PROVIDER**

UNIVERSITY of NEBRASKA-LINCOLN

IRS Continuing Education Provider (#NQ6J1) | Accredited with Nebraska Supreme Court MCLE Commission

The University of Nebraska does not discriminate based on any protected status. Please see go.unl.edu/nondiscrimination.

A PRIMER ON DIGITAL AND DATA SCIENCE ETHICS

Elementary schools and universities alike are turning to new technologies to assist in education. (In a post-COVID world, nearly every student in America has been in an online class or taken a virtual test with a virtual proctor.) However, in the push to keep up with a rapidly evolving technological landscape, the students' right to privacy seems to be dwindling. Or as Joel Reidenberg, the then-director of the Center on Law and Information Policy at Fordham Law School, described the information collected on a student through graduate school: "Just think George Orwell and take it to the nth degree. We're in an environment of surveillance, essentially. It will be an extraordinarily rich data set of your life."⁷ In educational spheres where student data is vacuumed up at an alarming rate—faces, voices, search histories, online shopping carts, location data, and more—consent becomes a troubling concept: Students are left with no choice but to allow this data to be collected as a condition for participation in education, with FERPA guidelines being undermined by behind-the-scenes data harvesting. This makes the push to answer fundamental questions about privacy as a civil rights issue even more urgent. We as a society need to figure out what lines need to be drawn about how student data may be used.

Which returns us to the larger ethical, legal, and programming challenge facing Americans: 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 obvious 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) and, to date, the U.S. has yet to pass any comprehensive laws regarding privacy similar to Europe's General Data Protection Regulation (GDPR).)

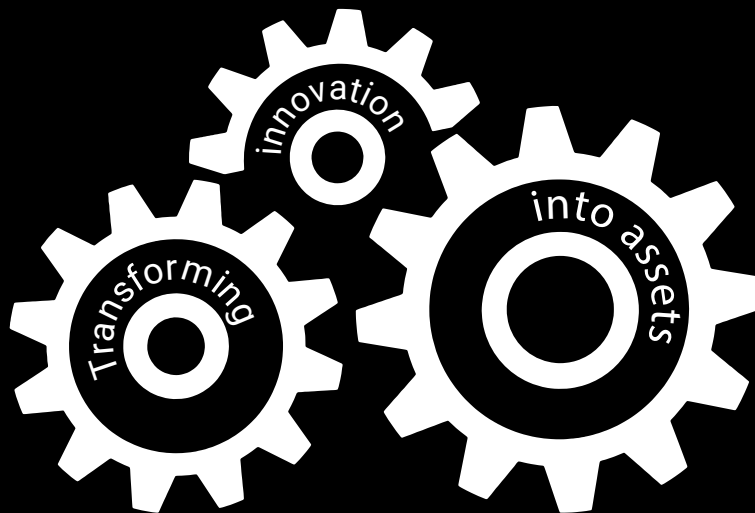
The notion of privacy as secrecy no longer meaningfully exists. As Justice Alito argued in *U.S. v. Jones*, if "an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," and almost all information about us is known or discernible, then privacy, as a legally protected concept, ceases 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, disintegrated to Fourth Amendment protection."⁸) The modern right to privacy will need to shift from a focus on "what is shared"—by acknowledging the reality that most information about us has already been collected—to a 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? Even



402.496.0300

| suiter.com

| Omaha, Nebraska



Patents | Trademarks | Copyrights

SUITER|SWANTZ
intellectual property

Hester Prynne was able to earn back the respect of her community.⁹ The notion of a statute of limitations on shunning, shaming, or cancellation should also be explored. In our view, we must create—in the U.S. and perhaps the world at large—a clear and unifying version of the right to be forgotten.¹⁰ As a society, we must build a collective post-digital ethos around privacy, and these new standards and community norms must include such quaint but critical notions as understanding, forgiveness, and grace.

The Challenges of 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. In terms of information and disinformation, this algorithmic gerrymandering determines what news, stories, advertisements, products, and political discourse we see online. In short, these algorithms can and do create our reality. (They put us into “filter bubbles” and create our current partisan divisions. This is why the IDH “bursts the bubble” by partnering with people and organizations on both sides of the informational divide.)¹¹ More precariously—because they are often invisible—these algorithms (which are, by default and design, often highly inaccurate and discriminatory) are increasingly used by prospective employers, landlords, businesses, health providers, police, schools, and government agencies.

The systems 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. And though the IDH focuses on algorithmic justice more broadly by looking not just at racial, gender, and disability discrimination by computer code, but also how known “error rates” wreak havoc on people’s lives, it is essential that the legal community understand that a system of technological discrimination (called, not hyperbolically, “Algorithmic Jim Crow” by Margaret Hu Professor of Law and Director of the Digital Democracy Lab at William & Mary Law School) is already underway. We will start with a general overview of algorithmic discrimination and how it happens, then explore relevant case studies where our technological civil rights are in true jeopardy: predictive policing, automated health care, employment AI, and the courts.

Algorithmic Bias 101

People too often treat algorithms like calculators and their decisions like solutions to math problems. 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 simply cannot be reduced to binary code

(i.e., algorithmic error rates); 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 (i.e., Algorithmic Jim Crow); or fail to holistically judge and evaluate an individual and their circumstances (as employees, defendants, patients, and suspects).

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.¹² 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.¹³ The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) algorithm is used to predict the likelihood of a criminal defendant’s recidivism.¹⁴ COMPAS predicted twice as many false positives for recidivism for Black offenders (45%) than for white offenders (23%).

Another issue with algorithmic decision making is that the algorithms are trained on flawed datasets. Algorithms are asked to predict the future based on the past. It should come as no surprise that a lot of racial, gender, and other biases are built into historical datasets. The use of these biased datasets is also called coding bias, and if left uncorrected, reinforces decades of marginalization and discrimination. When facial recognition programs often struggle to ‘see’ darker skin, how can their use be trusted in the hiring or interview process?¹⁵ An algorithm used to find more “high quality” or “successful” job candidates runs the risk of using a company’s hiring history to overlook qualified candidates who belong to historically marginalized groups.¹⁶

In addition to demanding transparency in the algorithmic process, human actors are needed to evaluate and revise automated decisions in essential spheres of human life. (Although, even with human oversight, we can still trust the machines too much. In 2021, researchers from the University of Georgia found that humans trust algorithms more than they trust other humans.¹⁷) What follows, for further thought and discussion, are some quick primers on how algorithmic bias is already happening.

Algorithms Making Policing Decisions

Predictive policing systems use data about where crimes have occurred in the past to predict how to deploy police forces. Many police departments use predictive policing algorithms to predict where crime is likely to occur. The technology surrounding predictive policing labels certain neighborhoods as “hotspots” or red zones. However, these neighborhoods are typically minority neighborhoods that are already subject to unwarranted and heavy police presence. The data fed to predictive policing algorithms is inevitably influenced by past

A PRIMER ON DIGITAL AND DATA SCIENCE ETHICS

issues with racist officers, practices, and—in some cases—even departments, meaning that officers and departments with good intentions often become unwitting instruments of racism and bias.¹⁸ A predictive policing algorithm may send officers to a predominantly Black neighborhood expecting to find trouble simply because of past racism that was, over time, incorporated into the department's policing practices.

Predictive policing algorithms can simply validate or amplify human biases and make it easier for law enforcement to reach reasonable suspicion standards, therefore justifying more police stops and harassment.¹⁹ Their use also begs the question: Is being labeled a high-risk individual by an algorithm enough to justify police surveillance? Predictive policing programs have a history of being used to target those individuals or groups police departments have considered undesirable.²⁰ Recent examples highlight how troubling the use of AI can be in criminal contexts. In Pasco County, Florida, the Sheriff's Office generated lists of people it considered likely to break the law, and then sent deputies to find and interrogate them, harass them, and humiliate them in front of their neighbors often without probable cause, a search warrant, or evidence of a specific crime.²¹ In Chicago, police have tried to curb gun violence by using an algorithm called the Strategic Subject List or S.S.L.²² The algorithm was developed in an attempt to maximize proficiency for the limited police resources. However, recent research and data suggest that the S.S.L. algorithm has

been a tool for the Chicago police department to target individuals who have not yet committed a crime.²³ These are just a couple of examples of how dangerous and unconstitutional predictive policing tactics can be.

Algorithms Making Health Care Decisions

Access to healthcare is a fundamental, and often life or death, human need. And yet, the same issues that plague algorithmic decision making in other contexts—error rates, systemic discrimination, re-purposing old data sets that have already failed a generation of marginalized citizens, and a lack of holistic understanding by the machine—are now emerging in health care contexts as doctors and hospitals increasingly turn to automated diagnostic and treatment protocols.²⁴

Racial biases in health care, both before and after algorithms, illuminate these issues. One of the most infamous examples of racism in medicine involved the Tuskegee Study, where a group of Black sharecroppers were denied informed consent and misled about the purpose of a study they participated in about as they participated in a study on untreated syphilis.²⁵ Even more tragically, once penicillin was found to cure syphilis, the study's participants were neither offered treatment nor were they told about the development of penicillin as a cure.



**Omaha
Community
Foundation**

Growing good,
together.

▶ ▶ ▶ Your philanthropic giving resource.

We partner with you and your clients as a part of the estate planning process to support your client's charitable goals both during life and as a legacy.

By gifting assets including publicly traded stock, closely held stock, and other non-cash assets to a Donor Advised Fund at the Omaha Community Foundation, your clients can support charitable causes while also reducing their tax liability.



Kelli Cavey, JD, CAP®
Vice President of Donor Services
402 614-9510
kelli@omahafoundation.org



Katie French McGill, JD, CAP®
Gift Acceptance Manager
402 884-1757
catherine@omahafoundation.org

A PRIMER ON DIGITAL AND DATA SCIENCE ETHICS

Sadly, racial biases in medicine persist. Forty percent of first- and second-year medical students believe that “Black people’s skin is thicker than white people’s.”²⁶ Black patients are 22% less likely than white patients to receive any pain medication.²⁷ Black women are three times more likely to die from a pregnancy-related cause than white women.²⁸

Tragically, algorithms seem to be “re-coding” this discrimination as they are used to make medical decisions. An in depth study of U.S. hospitals found that a widely used algorithm for medical care dramatically underestimated the health care needs of the sickest Black patients.²⁹ The algorithm was flawed as it was designed to use patients’ previous health care spending as a proxy for medical needs, ignoring the facts that poorer people are less likely to have access to health care or health insurance.³⁰ The FDA is investigating whether pulse oximeters may struggle to provide accurate reading for those with darker skin, leading to higher death rates from COVID-19 (and other illnesses) for people of color.³¹ People of color are also placed lower on transplant lists by algorithms, despite having higher rates of failure for certain organs.³² An algorithm widely used in U.S. hospitals to evaluate complex medical needs among patients was less likely to refer Black people to programs they needed than white people.³³ Racial biases are being programmed into medical devices, programs, and algorithms and putting human lives in danger.

Algorithms Making Employment Decisions

Companies are increasingly using artificial intelligence to determine whether individuals see job postings and to evaluate them if they apply.³⁴ When used to market specific job listings to certain people, these algorithms systematically deny people opportunities they didn’t even know existed. Is it constitutional to allow such an algorithm to silently

marginalize people without their knowledge?

When used to evaluate an employee mid-interview, these algorithms listen to applicants’ voices, watch their facial expres-



Do you have enough life insurance?

If you passed away unexpectedly, would your family be able to continue on financially? Or would they face drastic changes to their lifestyle — at the worst possible time?

The right life insurance can help assure your loved ones stay protected no matter what change comes your way. That’s why the Nebraska State Bar Association (NSBA) sponsors a Group Insurance Program designed exclusively for its members.

Act now to help ensure that your family has the financial security they need — when they need it the most.

Visit NEBarinsurance.com or call 1-866-236-8652 to learn more!*

*Including features, costs, eligibility, renewability, limitations and exclusions.

**Rates are expected but not guaranteed to not change during this period.



NEW YORK LIFE and the NEW YORK LIFE Box Logo are trademarks of New York Life Insurance Company. The NSBA Group Level Term Life Insurance Policies are underwritten by New York Life Insurance Company, New York, NY 10010, under Group Policy Forms GMR-FACE/G-30851-0 and GMR-FACE/G-30852-0.



Association Member Benefits Advisors, LLC.
In CA d/b/a Association Member Benefits & Insurance Agency
CA LIC #0196562 • AR License #100114462

Program Administered by AMBA Administrators, Inc.
97170 Copyright 2022 AMBA. All rights reserved.

Member advantages through this exclusive program include:

-  Your choice of benefit amounts up to \$1,000,000
-  Discounted rates for higher coverage amounts
-  Specially negotiated, locked-in** rates for 10 or 20 years, depending on which coverage you select
-  Tax-free benefit for your family. Please note that benefits received under this policy may be taxable. You should consult a personal Tax Advisor for further information.

GET MORE INFORMATION AND DOWNLOAD AN APPLICATION TODAY!



Sponsored by:




sions, gauge changes in expression and demeanor, see how they react to questions, and more.³⁵ This process is understandably controversial and poses a significant risk of coding racial, gender, disability, and other biases into the hiring process. But is it enough to tell applicants that the algorithm is being used? Should they be able to opt out in favor of a more traditional evaluation? HireVue, a leading company marketing artificial intelligence tools for use in hiring processes, was recently forced to stop using a candidate's facial expressions from video interviews as a factor in its assessments.³⁶

Algorithms can also be used to evaluate resumes, hypothetically reducing the number of overall interviews. However, an algorithm developed by Amazon to read resumes and select the best-qualified candidates quickly emerged as having been programmed to replicate existing hiring practices, such as preferring male candidates over non-male candidates and excluding female candidates.³⁷ Though this algorithm was eventually decommissioned, how many qualified and exceptional applicants were refused? How much of an impact did the decisions of that algorithm have on human lives?

Conclusion

Technological tools can be incredibly useful but must be used with caution. As attorneys, we must guard what remains of our clients' privacy zealously and act as a check on those who would abuse their data. As algorithms make more decisions that affect humans, those decisions will be subjected to legal challenges. As a profession, we will have to rethink our rules and practices in response. Our procedures, processes, and rules are designed for human actors. For example, how should courts deal with algorithmic evidence? How is a judge to deal with a situation where a witness (or declarant) is an algorithm? Should those who use algorithms to make decisions that affect people bear the burden of proving those decisions are being made fairly?

In our view, algorithmic error rates must be known and disclosed. Algorithmic systems must be trained on large, diverse, and representative data sets. Technological tools like algorithms must be designed thoughtfully, evaluated constantly, and audited regularly to ensure they are operating fairly. When technology is used against our clients, we must be educated about how it works and be prepared to push back when appropriate for the sake of a fair and just post-digital world. 

Endnotes

- ¹ Joseph Masi, Matthew Mandolfo, Madeleine Britto, Michael Bartz, William Harper, Kylie Karsky, Meagan Compton, and Emily Atamov are students at Creighton University, and research interns with the Creighton Business Law Research Forum, in collaboration with the Institute for Digital Humanity.
- ² See www.institutefordigitalhumanity.org for more victories and community education materials.

- ³ Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 Harvard L.R. 193 (Dec. 15, 1890).
- ⁴ Simon Hill, *How to stop apps from tracking your location in Android and iOS*, DigitalTrends, Mar 21, 2021, <https://www.digitaltrends.com/mobile/stop-apps-tracking-location/>.
- ⁵ The amount of data in the world was estimated to be 44 zettabytes (one sextillion bytes) at the dawn of 2020; by 2025, the amount of data generated **each day** is expected to reach 463 exabytes (one quintillion bytes) globally. As a point of reference, one estimate contends that **all words ever spoken** by human beings would amount to 5 exabytes. See Branka Vuleta, *How Much Data is Created Every Day?*, SeedScientific, Oct. 8, 2021, <https://seed-scientific.com/how-much-data-is-created-every-day/>; Tibi Puiu, *How big is a petabyte, exabyte or yottabyte? What's the biggest byte for that matter?*, ZME Science, Jan 29, 2021, <https://www.zmescience.com/science/how-big-data-can-get/>.
- ⁶ *U.S. v. Jones*, 565 U.S. __ (2012), slip op., Alito concurrence at 10.
- ⁷ Valerie Strauss, *Congress may create massive program to collect college student data*, Apr 4, 2022, <https://www.washingtonpost.com/education/2022/04/04/congress-student-data-collect-privacy/>.
- ⁸ *U.S. v. Jones*, 565 U.S. __ (2012), slip op., Sotomayor concurrence at 5.
- ⁹ Hawthorne, N. (1850). *The Scarlet Letter*. Boston, MA: Ticknor and Fields.
- ¹⁰ Everything you need to know about the "Right to be forgotten," GDPR-EU, <https://gdpr.eu/right-to-be-forgotten/?cn-reload-ed=1>.
- ¹¹ These filter bubbles, in addition to being politically dangerous, are also a form of trauma. See IDH Senior Researcher Hannah Grubbs, discuss this at <https://popularcultureandtheology.com/2021/09/22/wandavision-reality-and-the-filter-bubbles-that-control-our-minds/>.
- ¹² 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>.
- ¹³ Ariana Tobin and Ava Kofman, *Facebook Finally Agrees to Eliminate Tool That Enabled Discriminatory Advertising*, ProPublica, June 22, 2022, <https://www.propublica.org/article/facebook-doj-advertising-discrimination-settlement>.
- ¹⁴ 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>.
- ¹⁵ Thomas Reuters, *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>.
- ¹⁶ Miranda Bogen, *All the Ways Hiring Algorithms Can Introduce Bias*, May 6, 2019, <https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias>.
- ¹⁷ Bogert, E., Schecter, A. & Watson, R.T. Humans rely more on algorithms than social influence as a task becomes more difficult. *Sci Rep* 11, 8028 (2021). <https://doi.org/10.1038/s41598-021-87480-9>.
- ¹⁸ Diaz, A. (2021) "Data-Driven Policing's threat to our Constitutional Rights" Brookings Article, <https://www.brookings.edu/techstream/data-driven-policing-threat-to-our-constitutional-rights/>.
- ¹⁹ Asher, J. & Arthur, R. (2017) "Inside the Algorithm That Tries to Predict Gun Violence in Chicago" *The New York Times*, <https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html>.
- ²⁰ Kathleen McGroggy and Neil Bedi, *Targeted*, Tampa Bay Times, Sep 3, 2020, <https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/>.



A PRIMER ON DIGITAL AND DATA SCIENCE ETHICS

- ²¹ Nick Sibilia, Lawsuit: Florida County Uses 'Predictive Policing' To Arrest Residents For Petty Code Violations, *Forbes*, Apr 26, 2021, <https://www.forbes.com/sites/nicksibilia/2021/04/26/lawsuit-florida-county-uses-predictive-policing-to-arrest-residents-for-petty-code-violations/?sh=50c7a1c12d0f>.
- ²² Asher, J. & Arthur, R. (2017) "Inside the Algorithm That Tries to Predict Gun Violence in Chicago" *The New York Times*, <https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html>.
- ²³ *Id.*
- ²⁴ Katherine J. Igoe, Algorithmic Bias in Health Care Exacerbates Social Inequities — How to Prevent It, Mar 12, 2021, <https://www.hsph.harvard.edu/ecpe/how-to-prevent-algorithmic-bias-in-health-care/>.
- ²⁵ About the USPHS Syphilis Study, Tuskegee University, <https://www.tuskegee.edu/about-us/centers-of-excellence/bioethics-center/about-the-usphs-syphilis-study>.
- ²⁶ Janice A. Sabin, PhD, MSW, How we fail black patients in pain, Association of American Medical Colleges, Jan 6, 2020, <https://www.aamc.org/news-insights/how-we-fail-black-patients-pain>.
- ²⁷ *Id.*, citing Salimah H. Meghani, Eeeseung Byun and Rollin M. Gallagher, Time to take stock: a meta-analysis and systemic review of analgesic treatment disparities for pain in the United States, Jan 13, 2012, <https://pubmed.ncbi.nlm.nih.gov/22239747/>.
- ²⁸ Working Together to Reduce Black Maternal Mortality, Centers for Disease Control and Prevention, Apr 6, 2022, <https://www.cdc.gov/healthequity/features/maternal-mortality/index.html>.
- ²⁹ Carolyn Y. Johnson, Racial bias in a medical algorithm favors white patients over sicker black patients, *Washington Post*, Oct 24, 2019, <https://www.washingtonpost.com/health/2019/10/24/racial-bias-medical-algorithm-favors-white-patients-over-sicker-black-patients/>.
- ³⁰ Starre Vartan, Racial Bias Found in a Major Health Care Risk Algorithm, *Scientific American*, Oct 24, 2019, <https://www.scientificamerican.com/article/racial-bias-found-in-a-major-health-care-risk-algorithm/>.
- ³¹ Ben Leonard, Flawed oxygen readings may be behind Covid-19's toll on people of color, *Politico*, Jul 2, 2022, <https://www.politico.com/news/2022/07/02/flawed-oxygen-readings-may-be-behind-covid-19s-heavy-toll-on-minorities-00043282>.
- ³² Christensen, Donna M. et al. Medical Algorithms Are Failing Communities Of Color, Sept 9, 2021, <https://www.healthaffairs.org/doi/10.1377/forefront.20210903.976632/full/>.
- ³³ Ledford, Heidi, Millions of black people affected by racial bias in health-care algorithms, October 26, 2019, <https://www.nature.com/articles/d41586-019-03228-6>.
- ³⁴ Rebecca Heilweil, Artificial intelligence will help determine if you get your next job, *Vox*, Dec 12, 2019, <https://www.vox.com/recode/2019/12/12/20993665/artificial-intelligence-ai-job-screen>.
- ³⁵ Will Knight, Job Screening Service Halts Facial Analysis of Applicants, *Wired*, Jan 12, 2021, <https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/>.
- ³⁶ Jeremy Kahn, HireVue drops facial monitoring amid A.I. algorithm audit, *Fortune*, Jan 19, 2021, <https://fortune.com/2021/01/19/hirevue-drops-facial-monitoring-amid-a-i-algorithm-audit/>.
- ³⁷ Jeffrey Dastin, Amazon scraps secret recruiting tool that showed bias toward women, *Reuters*, Oct 10, 2018, <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>.

Below is the oath of admission, which is read aloud and repeated by attorneys when they are being sworn in.

Though the oath is short in length, it carries with it the tremendous responsibility that we as attorneys share. The NSBA reprints this oath as a reminder of the importance it carries and of the promises made by all Nebraska attorneys, starting with their first day in practice.

“

I do solemnly swear that I will support the Constitution of the United States, and the Constitution of this state, and that I will faithfully discharge the duties of an attorney and counselor, according to the best of my ability.

”