Potter Anderson Corroon LLP

YOUR DELAWARE ADVANTAGE

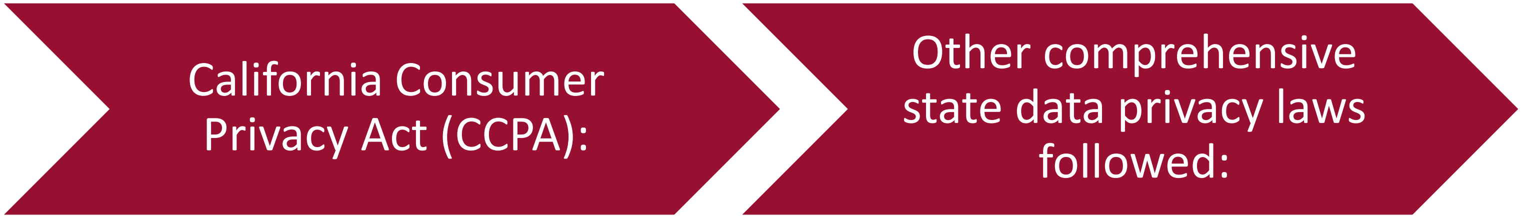
The new Delaware Personal Data Privacy Act and Recent Developments in Regulation of AI

Secure Delaware 2023 Cybersecurity Workshop

William R. Denny

October 24, 2023

Comprehensive State Data Privacy Laws



California Consumer Privacy Act (CCPA):

- Enacted in 2018
- First comprehensive state law
- Amended in 2020 by the California Privacy Rights Act (CPRA)

Other comprehensive state data privacy laws followed:

- 2021: Virginia and Colorado
- 2022: Utah and Connecticut
- 2023: Florida, Indiana, Iowa, Montana, Tennessee and Texas (and counting)
- Comprehensive privacy legislation is pending in 11 additional states

Scope and Applicability of DPDPA

- Delaware Personal Data Privacy Act applies to:
  - A “controller” who either
    - Conducts business in Delaware; or
    - Produces products or services targeted to residents of Delaware
  - **And** during the preceding calendar year
    - Controlled or processed personal data of not less than **35,000** Delaware residents (excluding payment transactions); or
    - Controlled or processed personal data of not less than **10,000** Delaware residents and derived more than **20%** of gross revenue from sale of personal data.
- Excludes: Governmental entities (except universities) and financial institutions
- Data exclusions: HIPAA data, scientific research data, consumer credit-reporting data, education data, employment-related information.
- CAUTION: Does NOT exempt nonprofits

Consumer Rights Vary by State

Right to access

Right to correct

Right to delete

Right to portability

Right to opt in for sensitive data processing

Right against automated decision-making

Private right of action

Right to opt out of certain processing (sales, targeted advertising, profiling)

Business Obligations

- Opt-in default for minors
- Notice / transparency requirements
- Responding to consumer rights requests
- Data protection assessments
- Prohibition on discrimination for exercising rights
- Purpose and processing limitations
- Data security
- De-identification of data

Major Challenges for Compliance

Scope and applicability – thresholds, entity-level and data-level exclusions

Definition of “Sale” including non-monetary consideration

Profiling and automated decision making

Global privacy controls / opt-out preference signals / universal opt-out mechanisms

Sensitive data: Opt-in or opt-out

Mandatory provisions in contracts with vendors/processors

Cure periods for violation and right of appeal

Action Items for Businesses

Assess	Assess compliance and gaps
Deploy	Deploy data management capabilities
Update	Update privacy policies and practices
Develop	Develop consumer request procedure
Update	Update vendor and supplier agreements
Implement	Implement reporting, recordkeeping and training
Boost	Boost data security and breach preparedness
Establish	Establish procedures for regular audit

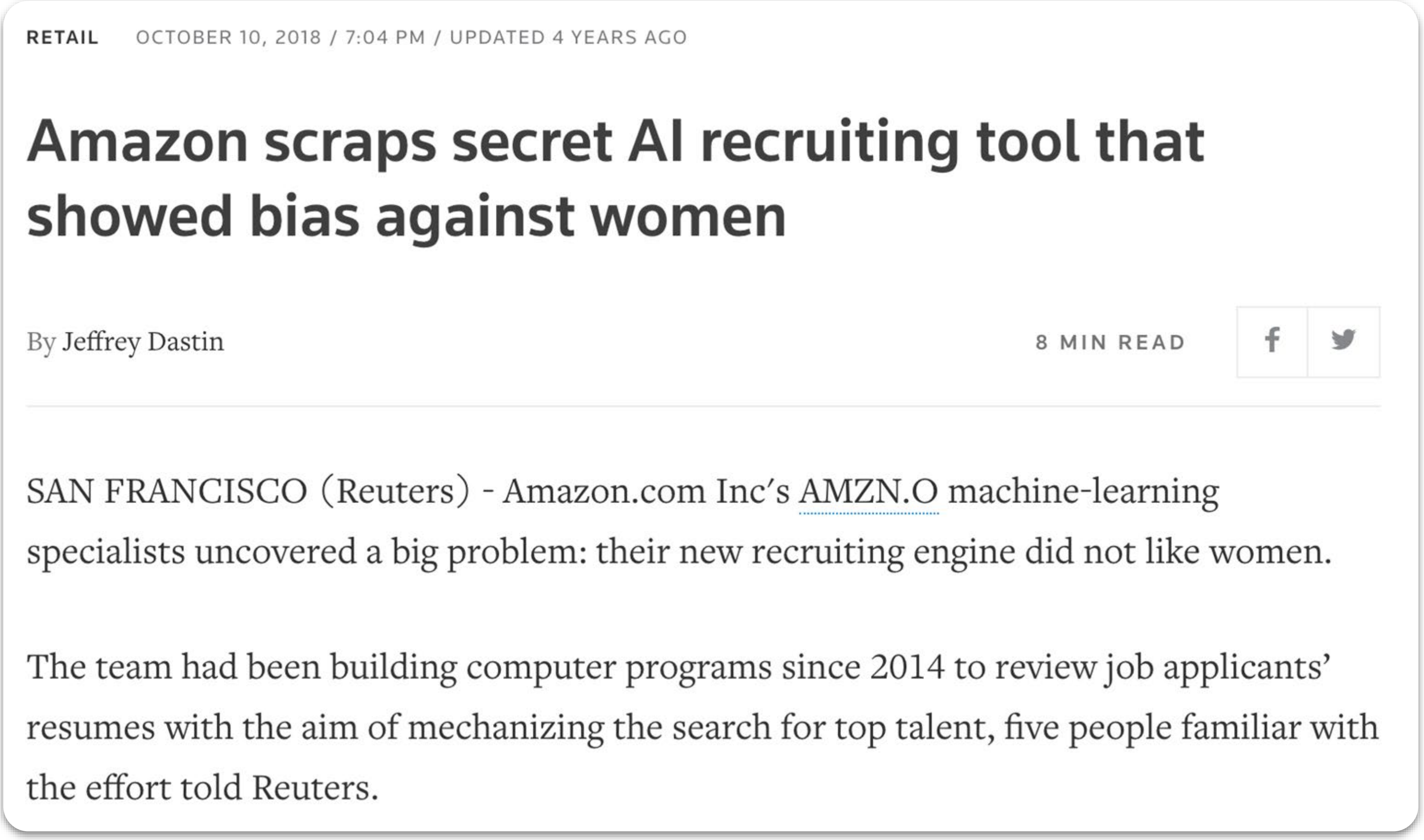
What is AI?

Astiein
Arssin
Antintinckinick
Acłfdinacvz
olc aliire lon fcgloyie anbinllvim
880 ʹO
18D 1EM
1,20ʜAcıral.

Issues with Generative AI

- Loss of Protected Data
- Intellectual Property Issues
- Accuracy: Hallucinations
- Explainability: “black box”
- Cyber: “synthetic media,” deepfakes
- Privacy and Bias: What is the training data

Scenario #1: Hiring Practices



RETAIL OCTOBER 10, 2018 / 7:04 PM / UPDATED 4 YEARS AGO

Amazon scraps secret AI recruiting tool that showed bias against women

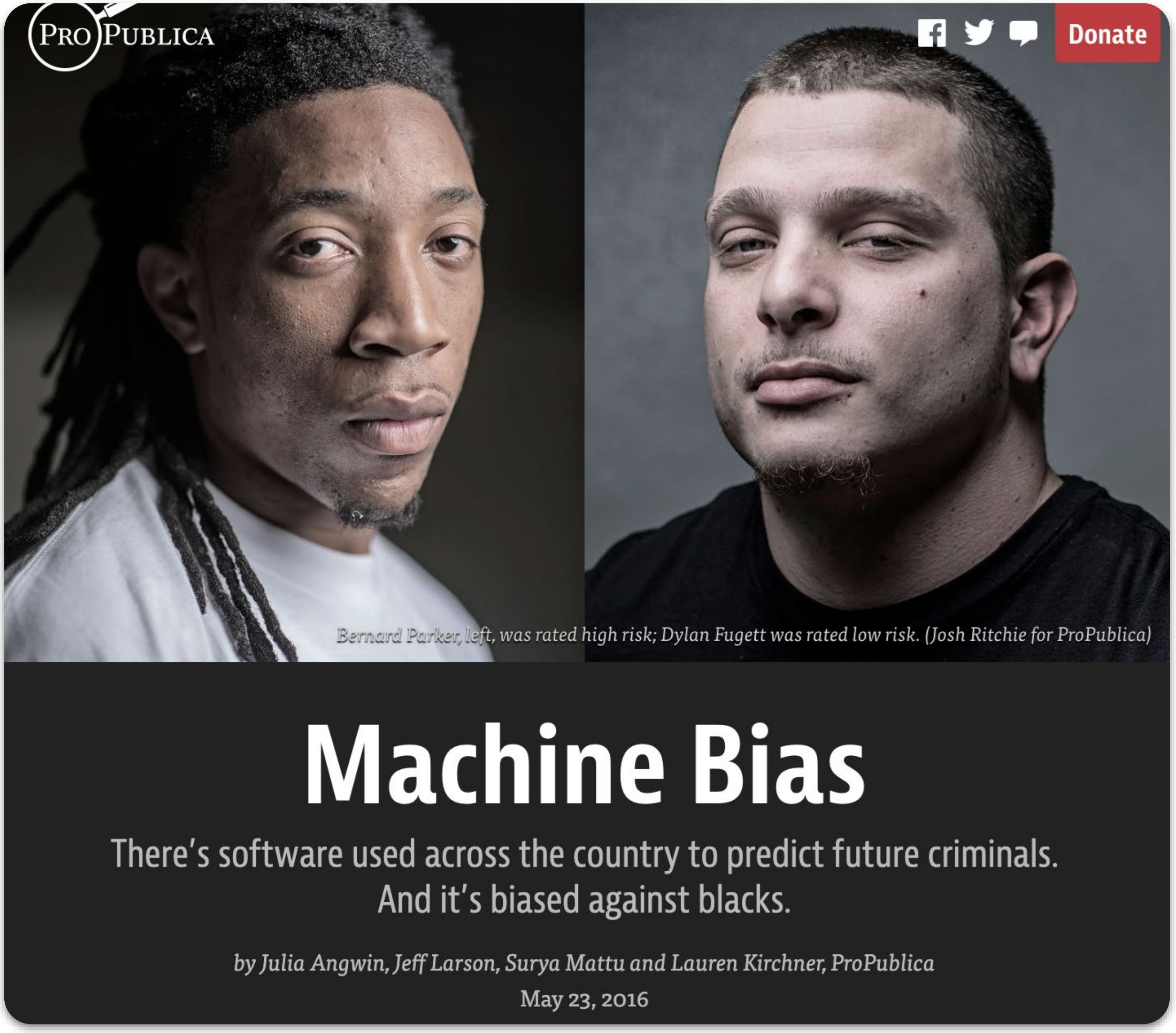
By Jeffrey Dastin

8 MIN READ

SAN FRANCISCO (Reuters) - Amazon.com Inc's AMZN.O machine-learning specialists uncovered a big problem: their new recruiting engine did not like women.

The team had been building computer programs since 2014 to review job applicants' resumes with the aim of mechanizing the search for top talent, five people familiar with the effort told Reuters.

Scenario #2: Recidivism



Bernard Parker, left, was rated high risk; Dylan Fugett was rated low risk. (Josh Ritchie for ProPublica)

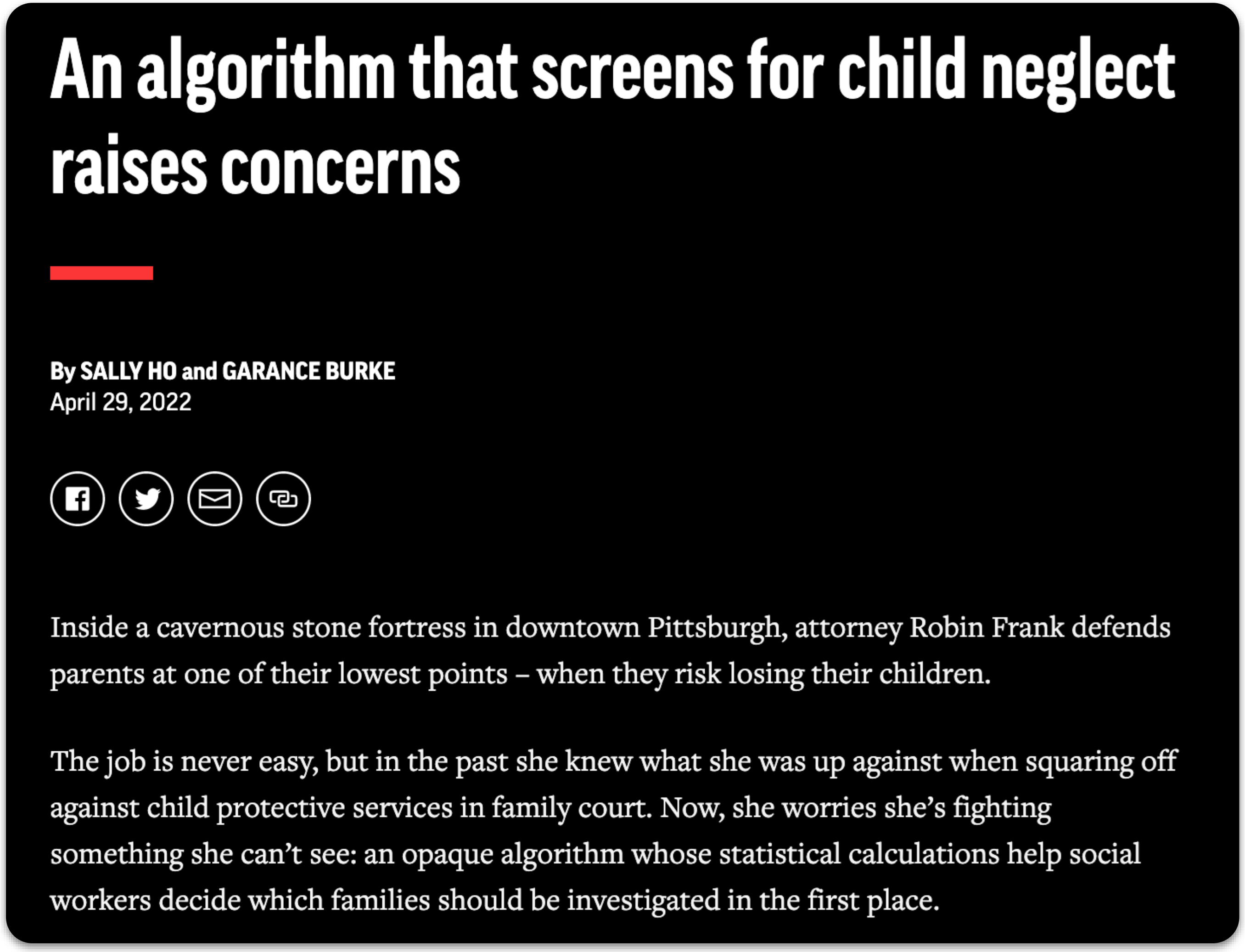
Machine Bias

There's software used across the country to predict future criminals. And it's biased against blacks.

by Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, ProPublica

May 23, 2016

Scenario #3: Child Protection



An algorithm that screens for child neglect raises concerns

By SALLY HO and GARANCE BURKE
April 29, 2022

Inside a cavernous stone fortress in downtown Pittsburgh, attorney Robin Frank defends parents at one of their lowest points – when they risk losing their children.

The job is never easy, but in the past she knew what she was up against when squaring off against child protective services in family court. Now, she worries she's fighting something she can't see: an opaque algorithm whose statistical calculations help social workers decide which families should be investigated in the first place.

Potter Anderson Corroon LLP

Scenario #4: Mata v. Avianca, Inc.

- In a personal injury matter, plaintiff’s counsel used ChatGPT for legal research
- ChatGPT fabricated cases to support plaintiff’s legal analysis
- Plaintiff’s counsel failed to check citations for accuracy
- Plaintiff then submitted non-existent judicial opinions and stood by the fake opinions
- Court imposed sanctions on plaintiff and his law firm
  - False and misleading statements to the Court
  - Plaintiff’s counsel doubled down and covered up

Copyright Issues

- Class Action Lawsuit alleges that AI generated images infringe on copyright because these models were trained using billions of copyrighted images without the consent of the artists.
- The complaint argues these new AI generated images should be treated as derivative works of the original artist that cannot be sold without infringing on the artists rights.
- AI image generators move to dismiss, arguing that:
  - AI generated images are not sufficiently similar
  - Artists do not identify specific image content they created
  - Artists do not identify specific AI generated image they allege is infringing

US Laws and Enforcement Affecting AI

AI is not a silo – it applies to a variety of services and products used by consumers

Joint statement by the CFPB, DOJ, EEOC and FTC in 2023 emphasized that aspects of AI systems are governed by existing law *(e.g.,* discrimination, deception, privacy)

The FTC enforces the Fair Credit Reporting Act, Equal Credit Opportunity Act, Children's Online Privacy Protection Act, and Section 5 of the FTC Act

Focus on enforcement relating to "high risk processing activities" – if using AI with sensitive data, make sure proper consents are in place or may have to delete algorithms that were created by using data unlawfully.

State Privacy Laws Govern AI

- State laws regulate the use of automated decision-making tools
  - They require proper disclosures, consents, opt-out rights, and impact assessments.
  - Focus on governing decisions that grant or deny financial services, insurance, housing, health care, employment, education or basic necessities.
- Additional disclosure requirements in Colorado:
  - The logic and training used to create AI tool,
  - Whether the AI tool has been evaluated for accuracy, fairness and bias, and
  - Why the AI tool must be used.

Draft AI Act – European Union

Unacceptable Risk

Systems that are considered a threat to people will be banned

High Risk

AI systems that negatively affect safety or fundamental rights will be assessed before being put on the market and throughout their lifecycle

Generative AI

Must comply with transparency requirements

Limited Risk

Must comply with minimal transparency requirements that would allow users to make informed decisions

The Future of AI Regulation

American Data Privacy and Protection Act (ADPPA) – potential federal law, likely to require:

- Engaging an external auditor to evaluate the design, structure and data inputs of AI tool to reduce risk of discriminatory impacts
- Evaluation would be required to be submitted to the FTC

SAFE Framework (Security, Accountability, Foundations, Explainability) would require disclosure of:

- Who trained the algorithm
- Who is intended audience
- Data source
- How the AIT tool arrives at its response, and
- Transparent and strong ethical boundaries

BLUEPRINT FOR AN AI BILL OF RIGHTS

MAKING AUTOMATED SYSTEMS WORK FOR
THE AMERICAN PEOPLE

OSTP

You should be protected from unsafe or ineffective systems.

You should not face discrimination by algorithms and systems should be used and designed in an equitable way.

You should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used.

You should know that an automated system is being used and understand how and why it contributes to outcomes that impact you.

You should be able to opt out, where appropriate, and have access to a person who can quickly consider and remedy problems you encounter.

AI and Commercial Transactions

Types of Agreements:

- Data licenses
- Platform and subscription agreements
- Service agreements

Contracting issues:

- Performance measures and compensation
- Use rights: track source, jurisdiction, data types, privacy restrictions, secondary uses, ownership
- Rights from data source: quality assurance, ongoing updates
- Proprietary vs. open systems
- Audit may be difficult or impossible
- Compliance
- Protect intellectual property rights

What Should Businesses Do?

Weigh	Weigh benefits of using AI against risks and cost of compliance
Map out	Map out how exactly the AI system works
Update	Update data inventory to understand what data is being input into the AI tool, how it is collected, why it is processed, how its output is stored and used.
Test and verify	Test and verify that tool works as expected, avoids bias
Govern	Govern the use of AI with internal policies
Manage	Manage risks and how to respond to incidents

Contact Us

William R. Denny

Direct dial: (302) 984-6039

wdenny@potteranderson.com

Potter Anderson & Corroon LLP
1313 North Market Street
Wilmington, DE 19801

potteranderson.com

Potter
Anderson
Corroon LLP