50 Shades of Data
September 14, 2023

ISSA
Information Systems Security Association
Colorado Springs Chapter

13th Annual
PEAK CYBER
Symposium

Agenda

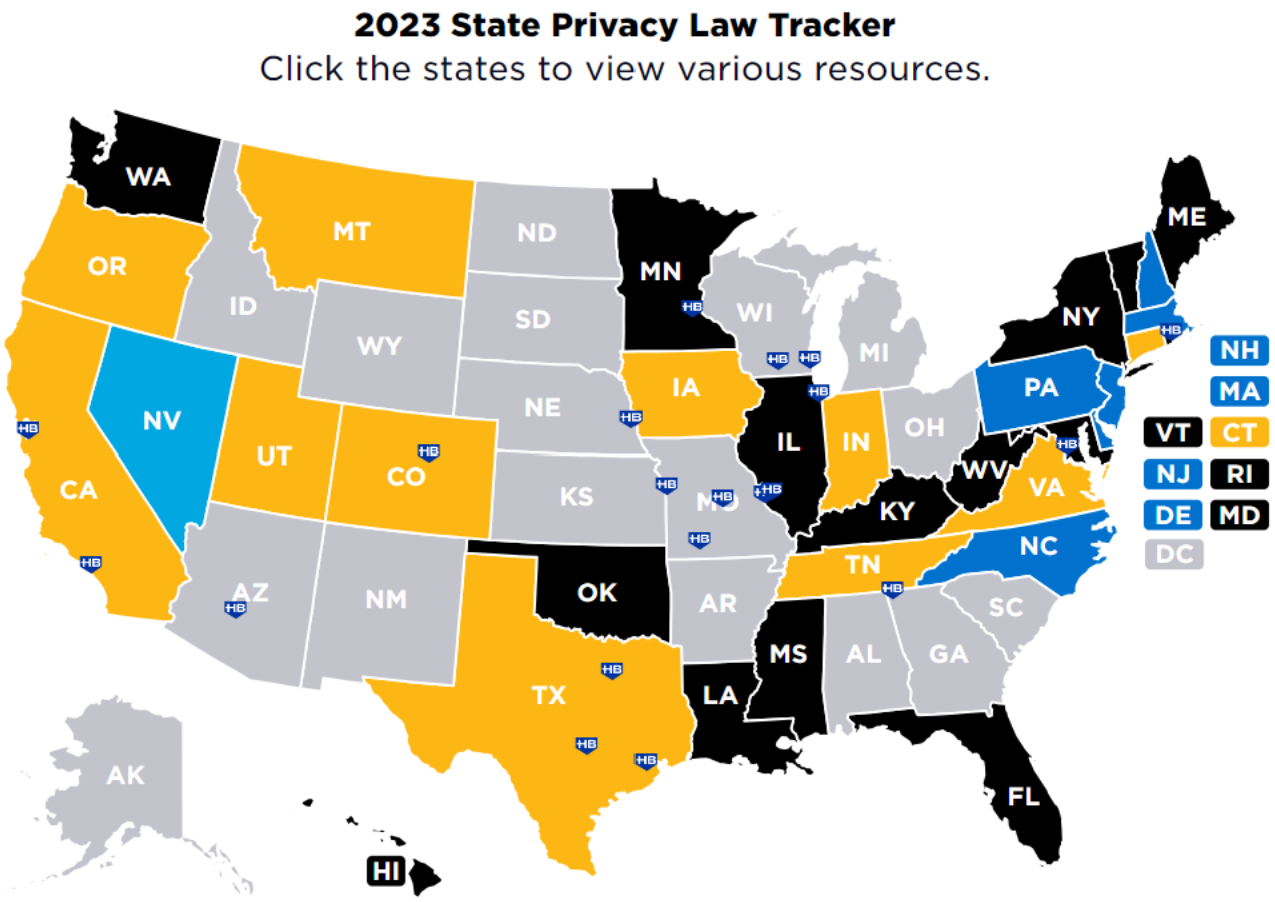
- Current US landscape
- 50 Shades of Data
  - Personal data, sensitive personal data, “regulated” data
  - Indirect data and inferences
  - De-identified personal data
- Is it really anonymous data?
- What’s the problem?
- What’s the harm?
- Next Steps

ISSA Colorado Springs Chapter

Disclaimer: I’m not a lawyer

13th Annual PEAK CYBER Symposium

Current US Privacy Laws



As of July 31, 2023

Note: Currently, only California covers HR and B2B data

- Enacted legislation
- Active legislation
- Did not pass in 2023
- Excluded legislation
- No bill proposed

HUSCH BLACKWELL

https://www.huschblackwell.com/2023-state-privacy-law-tracker

Eleven states enacted privacy laws by effective date

2020 California Consumer Privacy Act (CCPA)

01-01-2023 California Privacy Rights Act (CPRA)

01-01-2023 Virginia Consumer Data Protection Act (VCDPA)

07-01-2023 Colorado Privacy Act (CPA)

07-01-2023 Connecticut Data Privacy Act (CDPA)

12-31-2023 Utah Consumer Privacy Act (UCPA)

07-01-2024 Oregon Consumer Privacy Act (OCPA)

07-01-2024 Texas Data Privacy and Security Act (TDPSA)

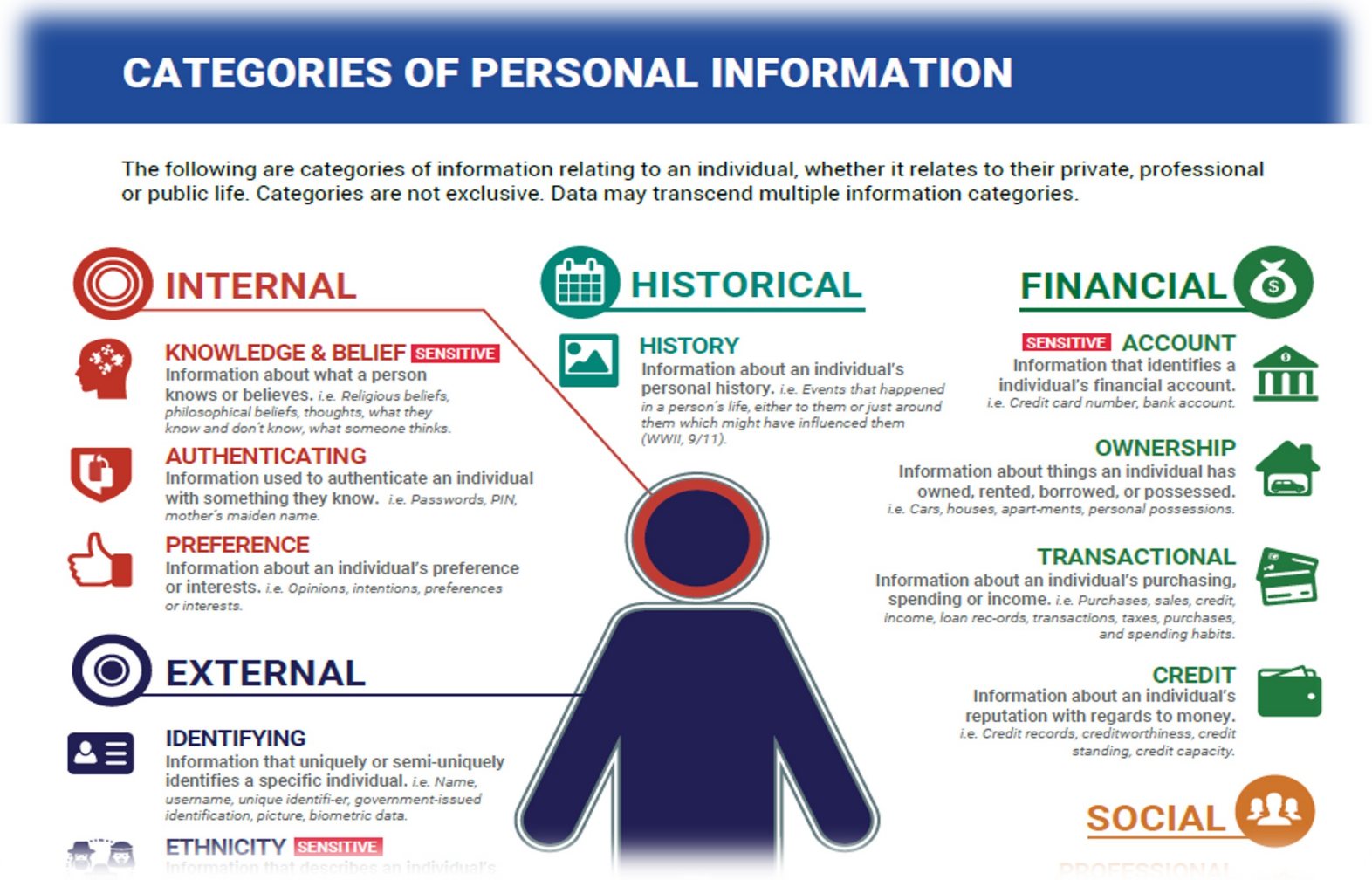
10-1-2024 Montana Consumer Data Privacy Act (MCDPA)

01-01-2025 Iowa Consumer Data Protection Act (IACDPA)

07-01-2025 Tennessee Information Privacy Act (TIPA)

01-01-2026 Indiana Consumer Data Protection Act (INCDPA)

“New” Definition of Personal Data



https://instituteofprivacydesign.org/resources/

Any data that is **linked or linkable** to an **identified or identifiable** individual.

Sensitive Personal Data

Biometrics* face, fingerprint, voice, iris, palm
Account Login and Password username, pin, password, authentication
Identifying SSN, Passport, Govt ID, National ID, Driver's License
Health diagnosis, test results, health insurance #, request for leave
Genetic data DNA (Genetic Information Nondiscrimination Act 2008)

DEI & Beliefs sexual orientation, gender identity, race, ethnicity, political party, religion, philosophical beliefs
Protected veteran status, citizenship status

Financial CC#, taxes, ownership of assets, purchase history
Location Precise GPS location*

Regulated Activities

- Is the personal data “shared” or “sold”? “Valuable Consideration”
- Is the data used for a “secondary use”?

- Are you “Profiling” people?
- Are you using it for “Targeted Advertising”? “Prediction”
- Are you using “Lookalike Models”?

- Using Artificial Intelligence or Machine Learning? “Legal Effect”
- Solely processing with “Automated Decision-Making?

Specific Laws Related to Children's Data

As of July 31, 2023

- Enacted legislation (7)
  - California
  - Utah
  - Texas
  - Arkansas
  - Louisiana
  - Florida
  - Connecticut
- Active legislation (3)
  - Massachusetts
  - New Jersey
  - North Carolina

- Some of the privacy laws include data on children*
- Take into consideration the age of the child - 13 and older or up to 16…17

ISSA Colorado Springs Chapter

Disclaimer: For informational purposes only, not legal advice.

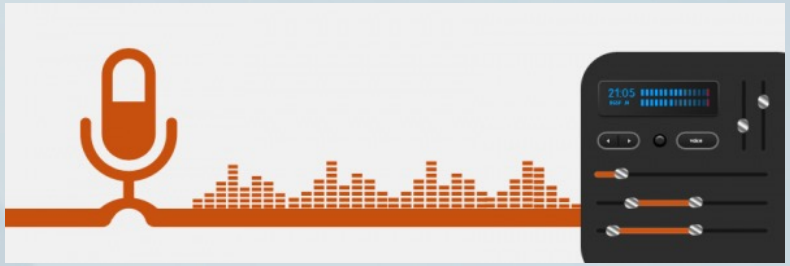
13th Annual PEAK CYBER Symposium

Biometric Information Privacy Acts

As of July 31, 2023

BIPA lawsuits

Biometric as sensitive personal data



- States – IL, TX, and WA
- Fingerprints
- Voice recognition software
  - Often used as a security measure and/or for identity verification

Disclaimer: For informational purposes only, not legal advice.

Privacy Impact Assessment – RISK (2023 laws)

Disclaimer: For informational purposes only, not legal advice.

Law	Effective Date	Language
GDPR *EU*	*05-25-2018*	*Article 35 - "…taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall…carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*
CCPA/CPRA - CA	01-01-2023	Section 1798.185(a)(15) Submit on a regular basis a risk assessment with respect to their processing of personal information
VCPA Virginia	01-01-2023	Section 59.1-576 Conduct a data protection assessment of each of the following processing activities involving personal data: 1. The processing of personal data for purposes of targeted advertising; 2. The sale of personal data; 3. The processing of personal data for purposes of profiling, 4. The processing of sensitive data; and 5. Any processing activities involving personal data that present a heightened risk of harm to consumers.
CPA Colorado	07-01-2023	Section 6-1-1309 A controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities involve personal data …that present a heightened risk of harm to a consumer.
CDPA Connecticut	07-01-2023	Section 8 A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer: 1. The processing of personal data for the purposes of targeted advertising; 2. The sale of personal data; 3. The processing of personal data for the purposes of profiling; and 4. The processing of sensitive data.
UCPA Utah	12-31-2023	None

Personal Data Exceptions

- Data about a company
- Aggregate personal data

- Regulated data (HIPAA and GLBA) – some maybe excluded
- De-Identified* personal data – mileage may vary
- Publicly available data but it's still "personal" – only in some laws is it not covered

Using Indirect Data to Identify

- Anonymity (2002)
  - Zip code, gender, and DOB (indirect) = ~87% of the US population

  https://aboutmyinfo.org/identity
- Unique in the Crowd (2013)
  - 4 geo location points = 95% of 1.5M people
- Strava Heat Map & the End of Secret Bases (2018)
  - Military bases detected

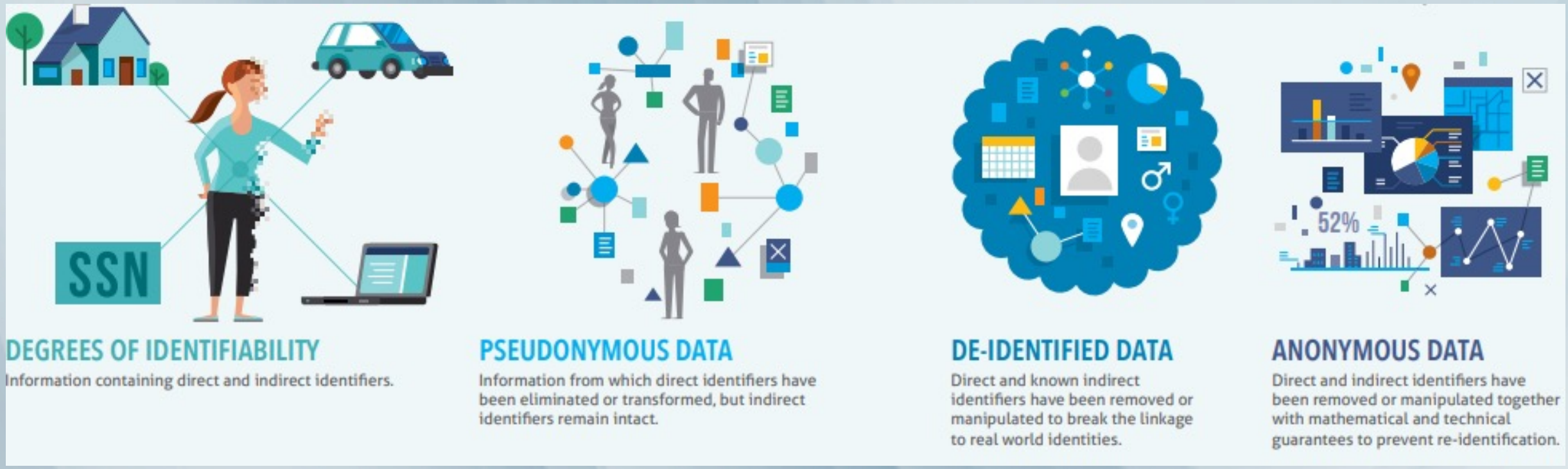
How anonymous is it?

Age Range	City	Weekly Salary	Title
18-35	Erie	Less than $1000	Manager
18-35	Erie	Less than $1000	Manager
18-35	Lafayette	Between $1000 - $5000	Manager
36-50	Erie	Between $1000 - $5000	Manager
36-50	Lafayette	Between $2000 - $5000	Director
36-50	Lafayette	Greater than $7000	CEO
50+	Erie	Between $3000 - $7000	Director

- Where does the CEO live?
- Sam is 25. What is his title?
- Bob is over 50. What's his title, where does he live, and how much does he make?

Degree of De-identification

Future of Privacy Forum



https://fpf.org/wp-content/uploads/2017/06/FPF_Visual-Guide-to-Practical-Data-DeID.pdf

ISSA Colorado Springs Chapter

13th Annual PEAK CYBER Symposium

Accuracy vs “Privacy”

Understand the **Data** so you can do the Trade off Analysis

- DOB
- Salary
- Exact Address
- Ethnicity (lots)

(German, South African, Indian, American, Dutch, Chinese, Japanese)

- Age or Month of Birth
- Salary Bands
- Zip code
- Race (limited categories)

(White, Black or African, Asian, Hispanic or Latino)

Fill in the blank “x” or Not “x”

We are **not** looking for

100% privacy

We want to **USE** the data but in a responsible and accountable way.

ISSA
Information Systems Security Association
Colorado Springs Chapter

13th Annual PEAK CYBER Symposium

What's the problem?

Imbalance of power. The burden should be on organizations and not on individuals.

- organizations are the ones collecting, using, disseminating, processing, and storing the personal data
- they are the only one that knows what data they have and how they will use your data

- privacy notices and 'choice' don't work
- Too long, too vague, too legalistic, sometimes just plain wrong

What's the harm?

- A "store" knowing you are pregnant before your parents do and you're 15 years old
- Websites diagnosing you with a disease before the doctor AND

  it raises your insurance premiums/you don't get a job/your profile is deprioritized
  - What you do - Change in mousing behavior could be a sign of early Parkinson's Disease.
  - What you search - Erectile Disfunction (ED) could be a sign of a serious medical condition.
  - What you watch - Your porn viewing habits (the type, time of day, location, type of device) could be used against you.
- Period tracking app data that can be used by authorities to determine if a women has had an abortion.
- Algorithms and Bias - Crime prediction software disproportionately targets low-income black and brown neighborhoods.

Systems contain data about people

Not just personal data

It’s your employees, friends, family, kids, spouse, partner, mother, father, sister, and brother

Next Steps

- ✓ Design privacy into our products and services
  - ✓ Defaults are sticky
  - ✓ KISS - People are not technical and sometimes naïve
- ✓ Stop collecting unlimited amounts of personal data
  - ✓ APIs and SDKs
  - ✓ Make sure you are doing PIAs
- ✓ Ask better questions and think outside the box

→ **Build a Privacy Program**

Record of Processing Activities (ROPA)
Data Mapping and Inventory
Data Subject Requests (DSR)
Incident Response Plan (IRP) that includes Privacy Incidents

Questions?

Thank you

Janelle Hsia
Janelle@privacyswan.com

PRIVACYSWAN
CONSULTING™

Resources

- Electronic Privacy Information Center (EPIC)
- Future of Privacy Forum (FPF)
- Institute of Operational Privacy Design (IOPD)
- International Association of Privacy Professionals (IAPP)
- Privacy Engineering Practice and Respect (PEPR) – conference
- Privacy Enhancing Technologies (PET) Symposium - conference
- Teach Privacy (Dan Solove) - conference
- The Coded Bias (2020) - movie
- The Great Hack Trailer (2019) - move
- The Social Dilemma (2020) - movie

Helpful Links

https://www.huschblackwell.com/2023-state-privacy-law-tracker

https://instituteofprivacydesign.org/resources/

https://fpf.org/wp-content/uploads/2017/06/FPF_Visual-Guide-to-Practical-Data-DeID.pdf

https://www.consumerreports.org/digital-security/online-security-and-privacy-guide/

https://privacy.commonsense.org/evaluations/1

https://www.humanetech.com/take-control

https://blog.google/products/search/new-options-for-removing-your-personally-identifiable-information-from-search

Definitions

Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.

"Share," "shared," or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business **to a third party for cross-context behavioral advertising**…including transactions… for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

Secondary use of information is when information is collected for one purpose but used something else like for marketing, upselling, hiring, firing, or performance analysis. It is really easy to see these data and then decide to use it for other purposes.

1. Cell phone numbers collected for MFA used for marketing
2. The company could use it against employees and the employees don't understand how it is being used against them.
3. An employee who was just curious looks at data they should ***not*** look at.

Disclaimer: For informational purposes only, not legal advice.

Definitions

Profiling analyzes aspects of an individual's personality, behavior, interests and habits to make predictions or decisions about them. You are carrying out profiling if you:

1. collect and analyze personal data on a large scale, using algorithms, AI or machine-learning;
2. identify associations to build links between different behaviors and attributes; create profiles that you apply to individuals; or
3. predict individuals' behaviors based on their assigned profiles.

Look-alike modeling is a process that identifies people who look and act just like your target audiences. This tool analyzes your seed audience, identifies some key characteristics and finds users who are similar to your target.

Definitions

Targeted advertising means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or *inferred* from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

"Targeted advertising" does not include:

1. Advertisements based on activities within a controller's own websites or online applications;
2. Advertisements based on the context of a consumer's current search query, visit to a website, or online application;
3. Advertisements directed to a consumer in response to the consumer's request for information or feedback; or
4. Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency.

Definitions

Automated decision-making is the process of making a decision by automated means without any human involvement. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. These decisions can be based on factual data, as well as on digitally created profiles or inferred data. Examples of this include:

1. an online decision to provide a loan;
2. an aptitude test used for recruitment or promotion that uses pre-programmed algorithms and criteria.

The Great Hack (2019)

They took your data and they controlled it.

5000 data points on every US voter

Are you “Persuadable”?

https://www.youtube.com/watch?v=iX8GxLP1FHo

The Social Dilemma (2020)

It's 'just' a design technique

Affect real behaviors and emotions

What if … **technology** creates mass chaos, loneliness, polarization, and more inability to focus on the real issues.

https://www.youtube.com/watch?v=uaaC57tcci0

Coded Bias (2020)

Joy Buolamwini

Pale-Male benchmarks

Power shadows

Gender shading

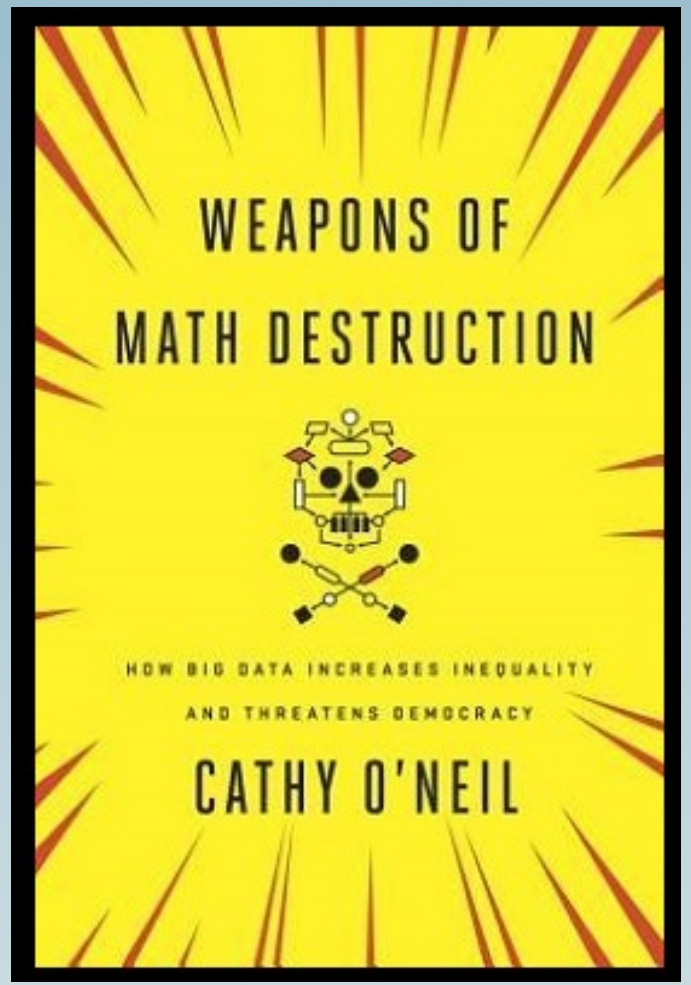
SafeFacePledge

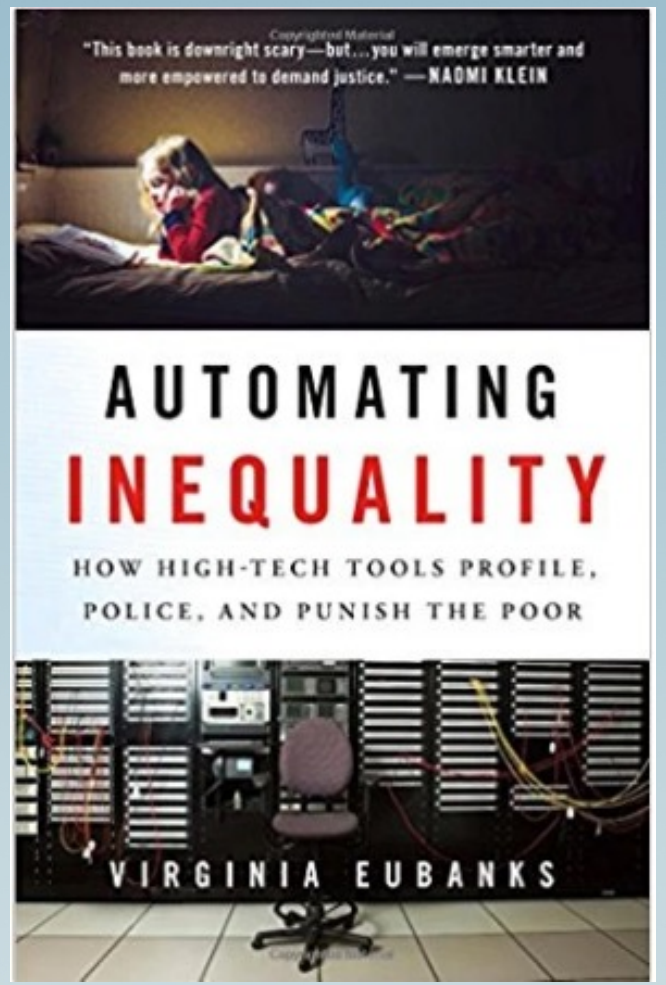
https://www.youtube.com/watch?v=eRUEVYndh9c

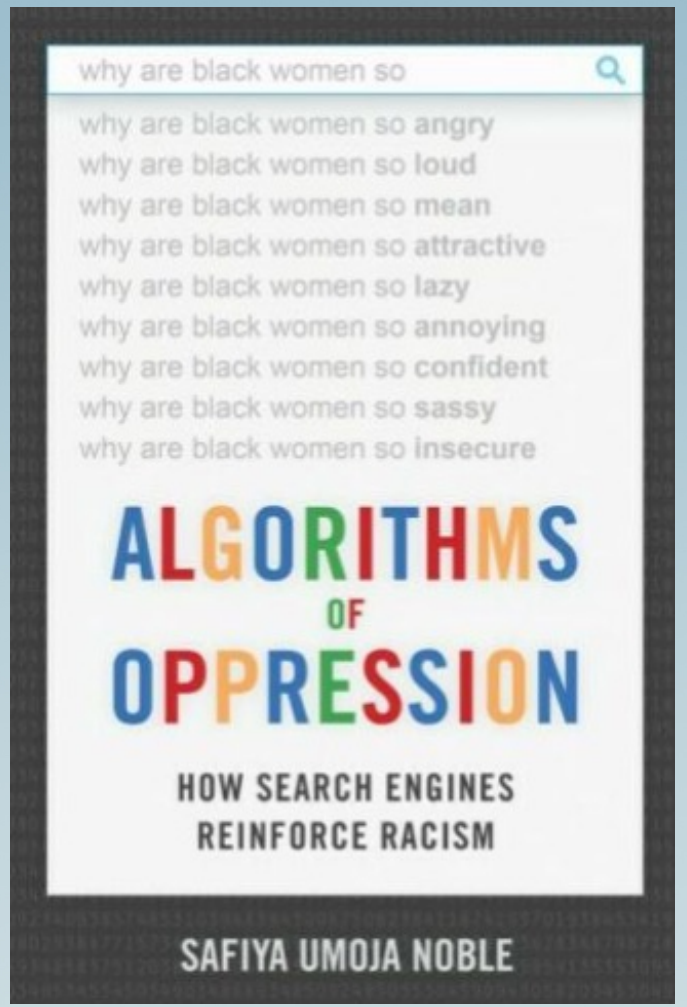
https://www.youtube.com/watch?v=jZl55PsfZJQ

ISSA Information Systems Security Association Colorado Springs Chapter

13th Annual PEAK CYBER Symposium


WEAPONS OF
MATH DESTRUCTION
HOW BIG DATA INCREASES INEQUALITY
AND THREATENS DEMOCRACY
CATHY O'NEIL


"This book is downright scary—but... you will emerge smarter and more empowered to demand justice." —NAOMI KLEIN
AUTOMATING
INEQUALITY
HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR
VIRGINIA EUBANKS


why are black women so
why are black women so angry
why are black women so loud
why are black women so mean
why are black women so attractive
why are black women so lazy
why are black women so annoying
why are black women so confident
why are black women so sassy
why are black women so insecure
ALGORITHMS
OF
OPPRESSION
HOW SEARCH ENGINES
REINFORCE RACISM
SAFIYA UMOJA NOBLE