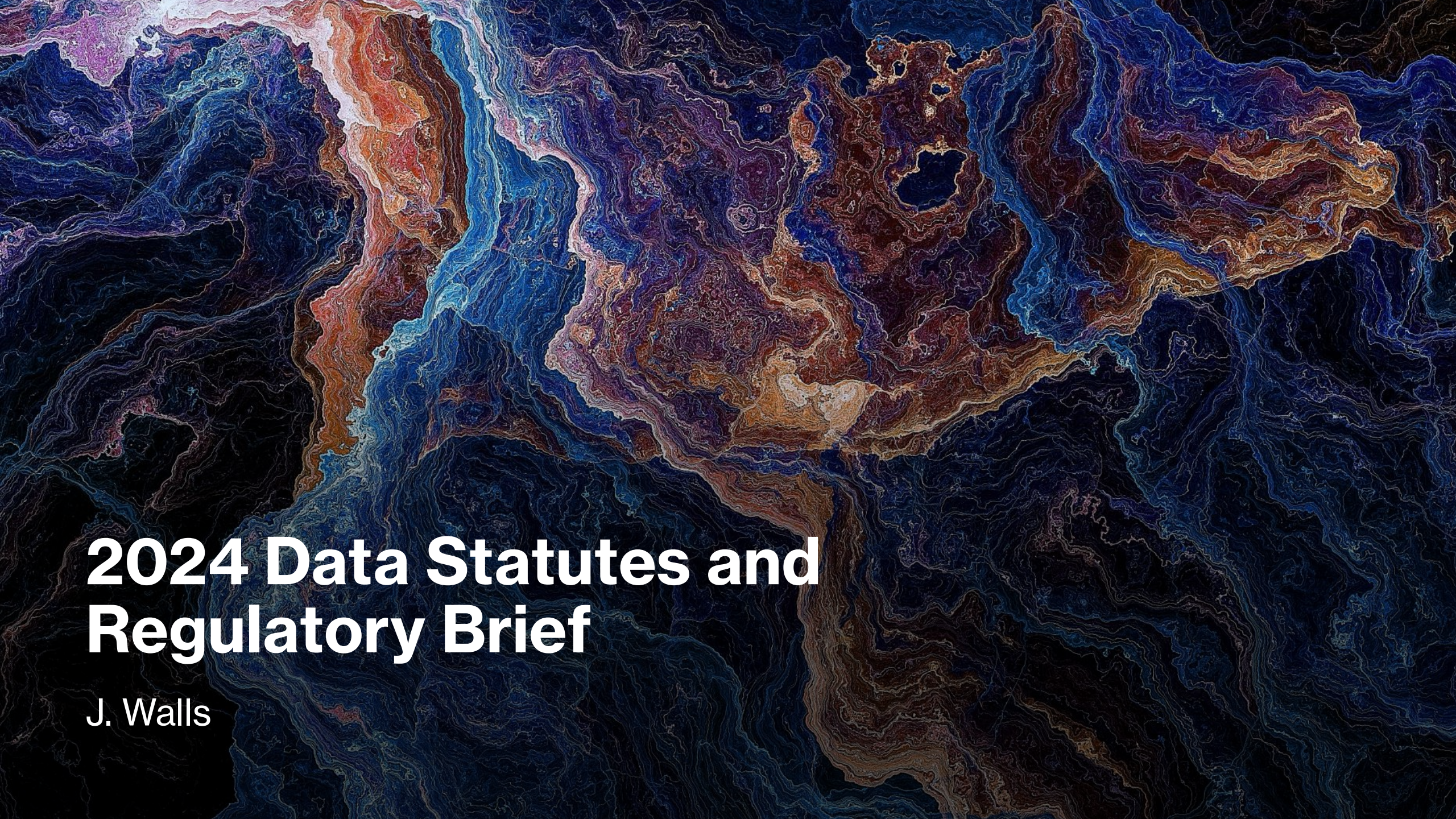


2024 Data Statutes and Regulatory Brief

J. Walls

Jonathan Walls

Masters of Science in Applied Statistics and Data Science student at APU

Professional experience collecting, preparing, analyzing, and reporting data

Have worked with such acronyms as CTC, CAEP, DOE, DOJ, NASP, NIH, NSF, & ABCDEFG

The Stakes

Data-Facilitated Human Rights Abuses: The Holocaust (1930’s-1940’s)

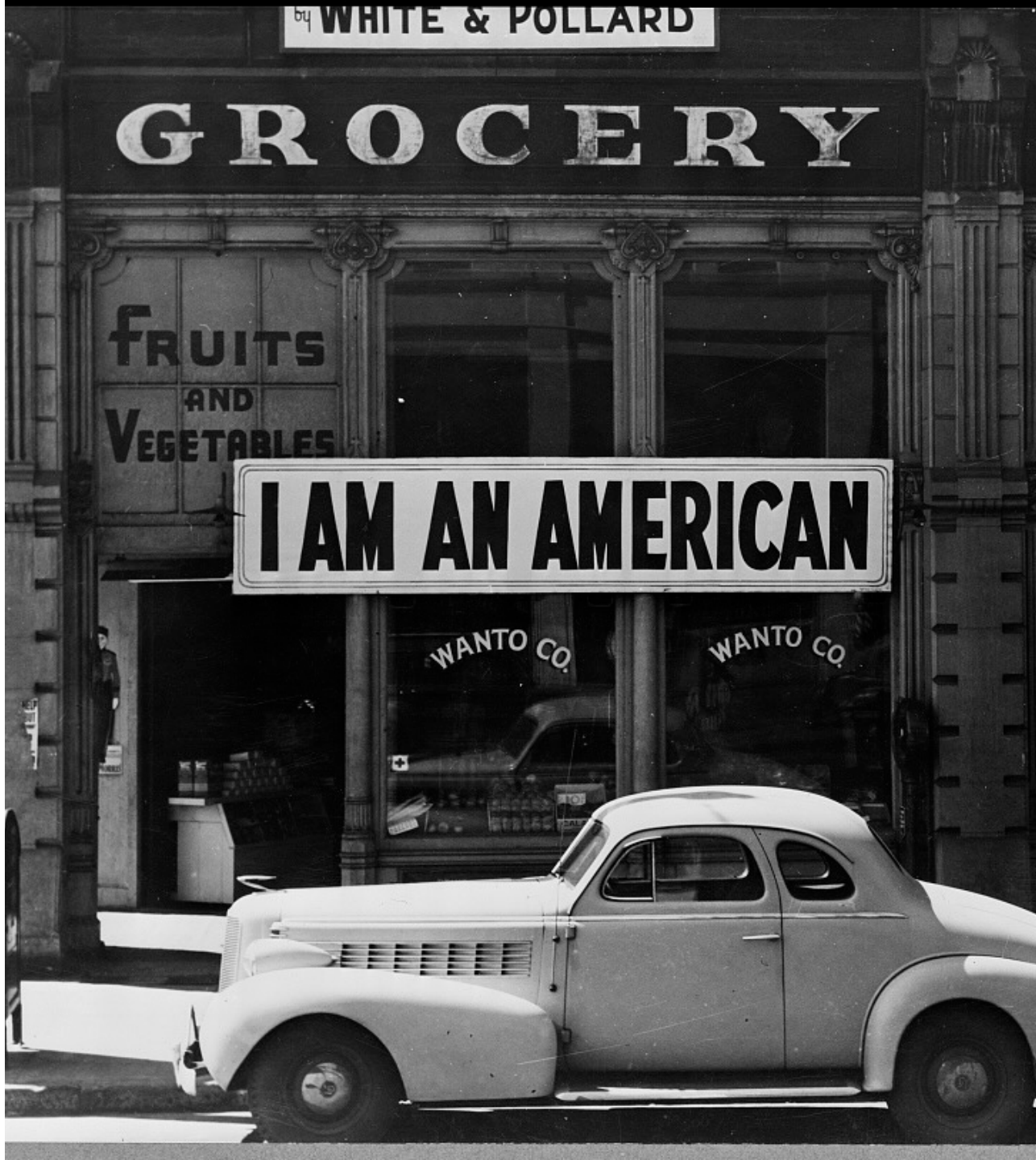
IBM punch card technology facilitated a complex national census that integrated demographic information, ghetto statistics, train logistics management, and concentration camp residency capacity.

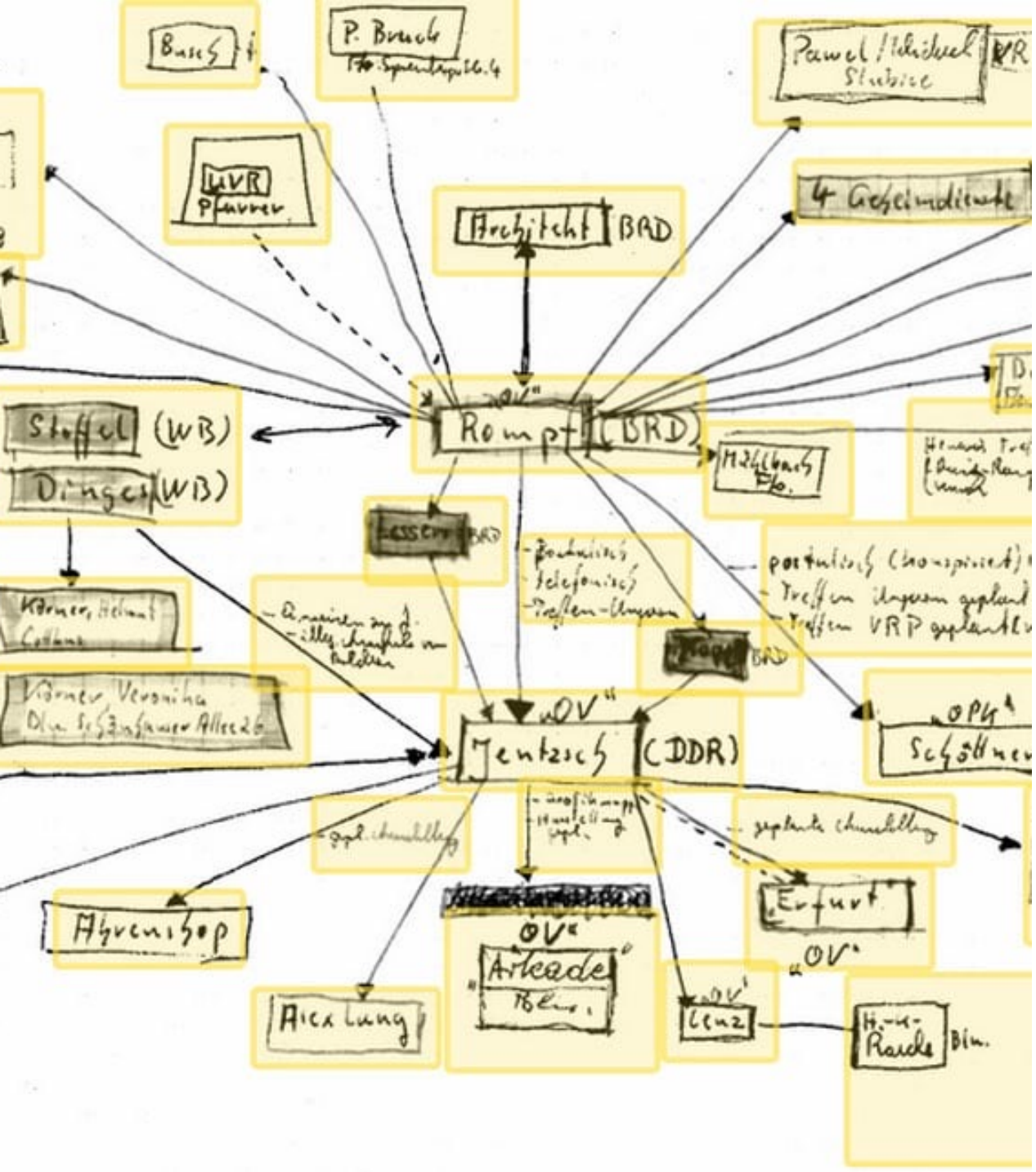
This facilitated the highly efficient systematic targeting of disfavored groups during the Holocaust resulting in the murder and genocide of 6 million European Jews, 2/3rds of their continental population. Disfavored groups also included political dissidents, gay men, disabled persons, ”asocials”, Soviets, Poles, and black German citizens.

Data-Facilitated Human Rights Abuses: Japanese Internment Camps (1940's)

In 1942, Franklin D. Roosevelt issued executive order 9066 to forcibly relocate over 100,000 Japanese first (Issei) or second generation (Nisei) American citizens into concentration camps.

The 1940 US Census collected data that was disaggregated to identify and locate internment candidates. The variables used included race/ethnicity ("color"), birthplace, home values, farm ownership, members of the household, additional places of residence, employment details, income, and more. This data set was also used to assume control of property, family farms, and businesses.





Data-Facilitated Human Rights Abuses: The Stasi (1950-1989)

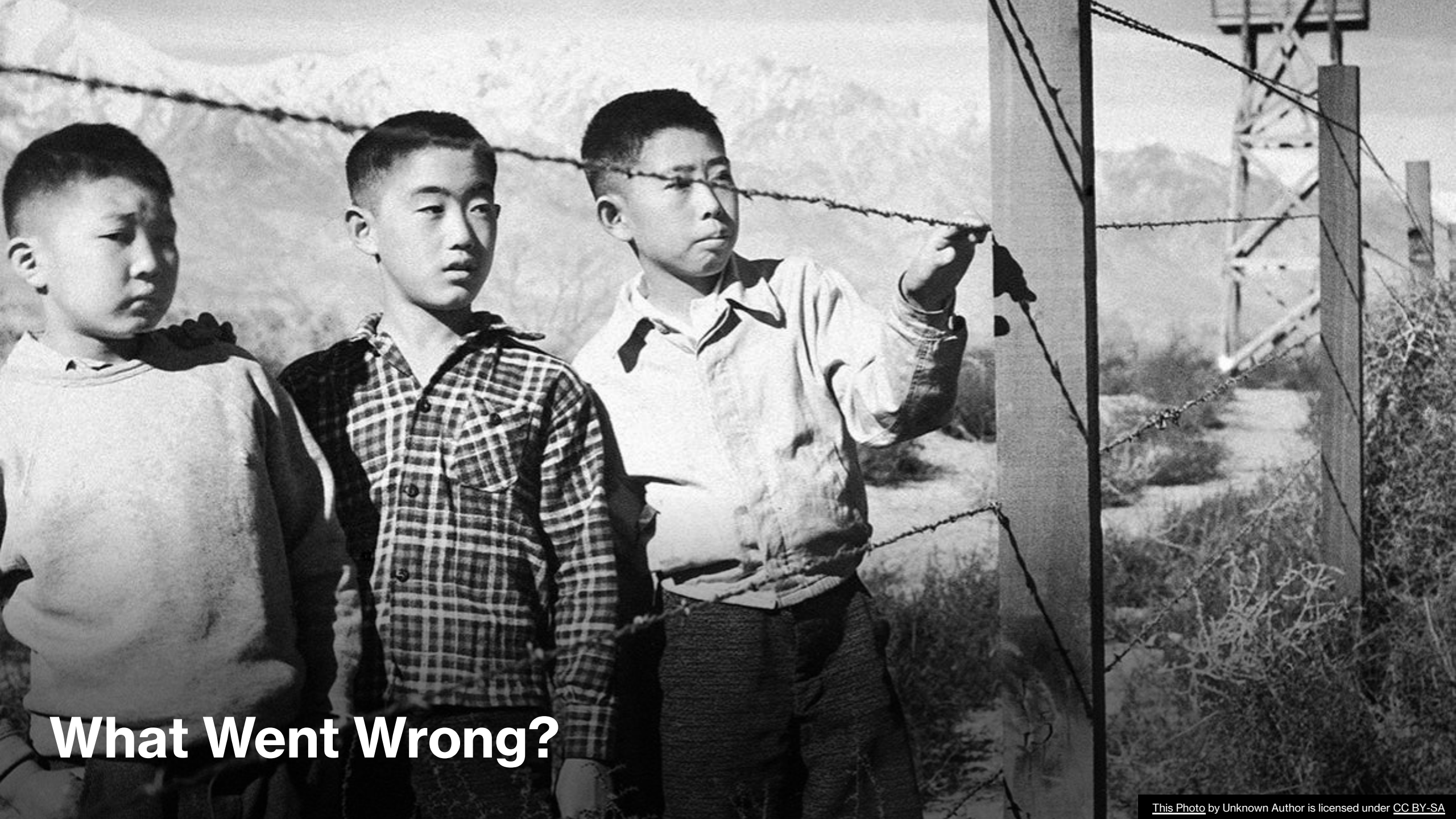
The Communist East German Ministry for State Security, (Stasi) spied extensively on their own citizens, collecting and archiving records accumulated via surveillance for over 5.6 million people with 69 miles (111 km) worth of files end-to-end.

The surveillance generated observational data that was complex but crudely organized. It was analyzed for the purpose of identifying and suppressing political opponents/ dissidents who were often beaten into false confessions, tortured, kidnapped, and/or killed.

Data-Facilitated Human Rights Abuses: Apartheid (1948-1994)

The South African government used the data collected by the Population Registration Act of 1950 (PRA) to segregate its citizens.

The PRA created a detailed ethnotypic data set including head hair, body hair, skin color, facial features, home language, and eating/drinking habits. The features in this data set led to the creation of the stereotypical racial categories that were used to enforce Apartheid segregation policies and are still in use today by the South African government.



What Went Wrong?

Characteristics of Ethical Failures in Data Usage

- Conflict of Interest
- Lack of Consent
- Violation of Privacy
- Lack of Transparency
- Bias/Discrimination
- Data Security Neglect
- The “work-around” (bypassing or ignoring regulation)

Ethical Failures in Data Usage: Conflict of Interest (COI)

General Context

These are domain/sector specific and involve the relationship between one entity (or individual) and another entity (or individual). Laws and regulations may apply depending on the domain/sector of the business and the domain/sector of the client. Corporate involvement in research publication (or the suppression of research publication) regarding their own products is a common source of COI. A commonly ignored COI: government research funding priorities published every cycle have the effect of soliciting research with de facto predetermined outcomes...they support political policy goals.

COI Prevention for Data Professions

Conflict exists where the data professional's work for one client is substantively altered, limited, or made substandard by their work for or relationship with another client or entity. Any conflicts of interest should be disclosed both internally by administrative processes that document the parties involved, the nature of the conflict, and the potential ramifications. Any publications should acknowledge and elucidate any conflicts of interest.

Ethical Failures in Data Usage: Lack of Consent

General Context

Laws and regulations may apply depending on the domain/sector of the entity and the domain/sector of the client. Bypassing consent is a common ethical lapse in historically significant human rights violations such as the the Tuskeegee syphilis experiment that collected unconsented health data for 40 years from 1932 to 1972.

Lack of Consent Prevention for Data Professionals

This is defined by the confluence of federal and state law (CCPA and CPRA). In some cases consent is assumed, where not explicitly covered by law. An affirmative, informed consent that covers every aspect of data usage enumerated in state and federal law should be acquired and documented according to established processes that are uniformly applied to all clients, comply with associated laws, and subjected to annual audit and review, the products of which may be required to be submitted to regulatory agencies.

Ethical Failures in Data Usage: Violation of Privacy

General Context

In addition to the CCPA and CPRA, regulatory background for California privacy law begins with the 4th Amendment to the US Constitution and incorporates domain-specific acts such as the Federal Trade Commission Act (FTC), Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act (CFAA), HIPAA, and COPPA. Google settled with the FTC for $170 million in a case brought because YouTube collected data from children for use in targeted advertising, violating COPPA.

Violation of Privacy Prevention for Data Professionals

Entities should create a culture of privacy sanctity evidenced by regularly-maintained policies regarding data collection, use, and protection. Having a strong consumer response process that is reviewed for continuous improvement can identify weaknesses and fortify strengths. Other measures that protect entities from Violations of Privacy include formal data mapping, minimization strategies, encryption, access controls, employee training, risk assessments, and breach notification protocols.

Ethical Failures in Data Usage: Lack of Transparency

General Context

Transparency regulations in California are defined by the CCPA and CPRA in addition to FTC regulations against deceptive practices. Consumers must be provided with info regarding the data collected, its purposes, opportunities to consent where appropriate, and notice to opt out of the sale of data to third parties. Federal government agencies must comply with Freedom of Information Act (FOIA) requests regarding data. The Supreme Court case *Missouri v. Biden* revealed a previously hidden vast network of government agencies and government-funded NGO's who collected the personal information of Twitter and Facebook users engaged in disfavored political speech and used it to pressure sites into removing or hiding posts by those users. This was not disclosed by Twitter or Facebook.

Lack of Transparency Prevention for Data Professionals

Transparency can be a safeguard and a self-correcting mechanism against other ethical failures such as the publication of misleading/false information, violation of privacy, conflicts of interest, bias/discrimination, and more.

Ethical Failures in Data Usage: Bias/ Discrimination

General Context

In addition to the applicable protections in the CCPA and CPRA, federal and state protected class characteristics are defined by the Fair Credit Reporting Act (FCRA), Equal Opportunity Act (ECOA), the Unruh Civil Rights Act, California Fair Employment and Housing Act (FEHA). In modern context, predictive policing tools (algorithms) have come under scrutiny for their tendency to perpetuate and even exacerbate existing racial discrimination.

Bias/Discrimination Prevention for Data Professionals

Creating review committees comprised of individuals with differing cultural, ethnic, and ideological perspectives can help identify blind spots and patterns of bias. One of the most under-addressed sources of bias in industry is ideologically-based. Preventative practices include transparency, employee training that reinforces strong policies reviewed by risk management/legal, internal bias mitigation (including audits and statistical analysis), and external audits.

Ethical Failures in Data Usage: Data Security Neglect

General Context

The Federal Information Security Modernization Act (FISMA), Gramm-Leach-Billey Act (GLBA), FERPA, HIPAA, CCPA and CPRA all contain provisions that effect how an entity can handle data security. In 2017, data security neglect at Equifax led to a severe breach. Personal Information was exposed including social security numbers, drivers' licenses, birth dates, addresses, etc. Equifax had not updated its systems to patch a security flaw in Apache Struts that had been available for two months.

Data Security Neglect Prevention for Data Professionals

Data security can be reinforced with administrative processes, beginning with the creation of strong policies and procedures approved through risk management/legal and reinforced by generous employee training. Those policies and procedures should be proactive and include comprehensive risk assessments, an incident response plan, and thorough compliance documentation.

Ethical Failures in Data Usage: The "Work-Around"

General Context

The CCPA and CPRA establish penalties and fines for intentional ($7500 per violation) and unintentional ($2500 per violation) violations of law. Domains such as Health Care, Education, Finance, etc, are each accountable to additional laws from domain-specific legislation such as HIPAA, FERPA, and the FTC. From 2002 to 2016, Wells Fargo employees were driven by sales incentive to create customer credit card accounts without their consent. This was in spite of the commonly understood consent laws of the time. The result was a bevy of civil claims and a $3 billion fine.

Work-Around Prevention for Data Professionals

Entities are required to prove their compliance to the CCPA and CPRA. It is ideal to begin with strong policies and procedures that address all the general principles and rights of data subjects and then to build those out with training, stringent and detailed documentation,

Is Data Regulation a New Issue?

Data Regulation Evolves from Trigger Events

Privacy/Individual Rights/Data protections in societies typically evolve over time from egregious and continued civil/human rights violations that include data abuses

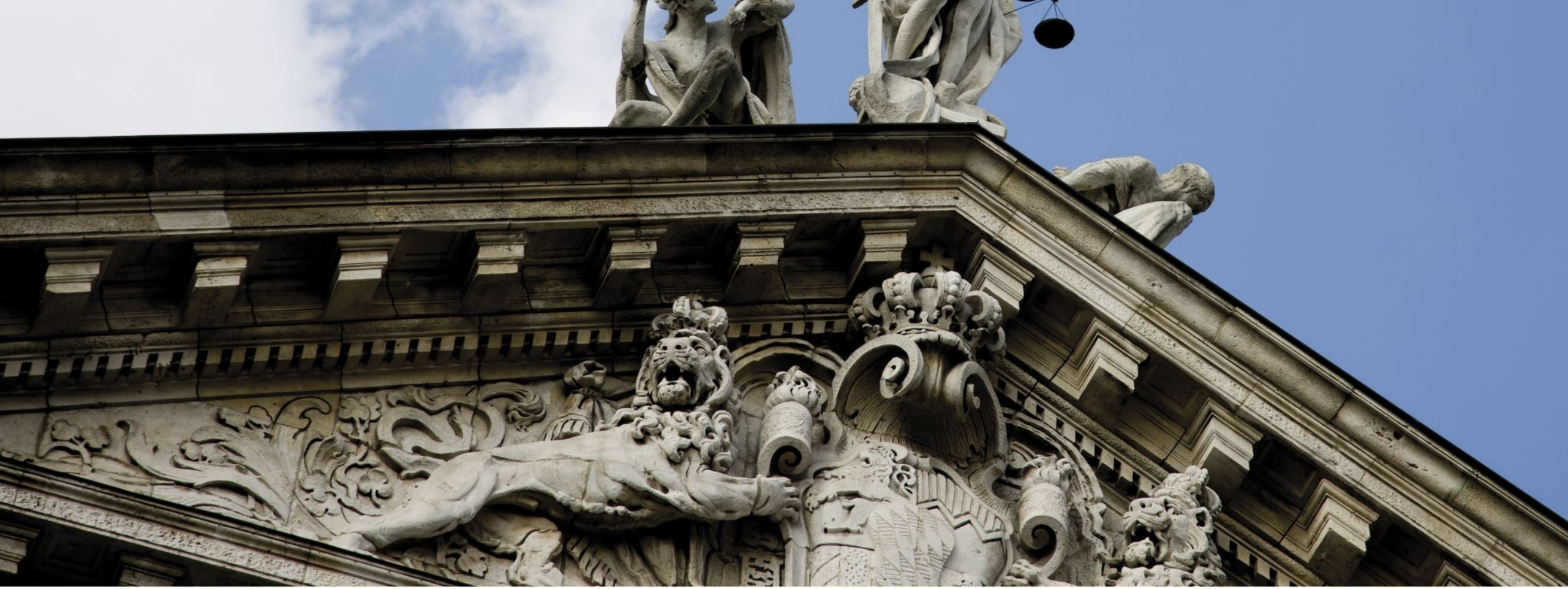
- USA: American Revolution
- EU: Nazi Germany and Communist East Germany

American Revolution and Subsequent Legal Implications

- **1789 – United States Constitution's First, Third, Fourth, and Fifth Amendments** Create the Foundation for Rights to Privacy
- **1890 – Supreme Court Justice Louis Brandeis argues for the right to privacy** attached to these amendments in the famous "Right to Privacy" law review published in the 1890 Harvard Law Review related to the invasion of new technology into private life: pictures
- **1914 – Federal Trade Commission Act (FTCA)** outlaws unfair/deceptive commercial practices. FTC is typically the federal agency involved with privacy issues and enforcement of regulations
- **1960's -1970's – Several Supreme Court rulings** related to intimate practices, unlawful searches and seizures
- **1973 - Records, Computers and the Rights of Citizens: Report of the HEW Advisory Committee on Automated Personal Data Systems -** The report was the origin of *Fair Information Practices*, a set of principles that formed the basis for modern privacy legislation.

American Revolution and Subsequent Legal Implications

- **1974** - **Family Educational Rights and Privacy ACT of 1974 (FERPA)**: safeguards the privacy of student education records**. Privacy Act of 1974:** Code of Fair Information Practice on federal collection, maintenance, use, and dissemination of personally identifiable information.
- **1996 – Health Insurance Portability and Accountability Act (HIPAA):** protects personally identifiable information within healthcare and insurance industries
- **1998 - Children's Online Privacy Protection Act (COPPA**) – protects children under 13 from data collection
- **2001 – Patriot Act –** Subjects American citizens to national security tools used in foreign warfare



The European Path to the General Data Protection Regulation (GDPR) Began with Nazi Germany and Continued Momentum Due to Abuses in Communist East Germany

- Nazi Germany (1933-1945)
  - Collected information to document ancestry and affiliations. Famously resulted in targeting, abuse, and murder.
- Communist East Germany (1949-1990)
  - Secret Police

The European Path to the General Data Protection Regulation (GDPR)

- **1978 -** Germany enacts first national law governing data: their **Federal Data Protection Act**
- **1983 – German court system (Federal Constitutional Court) institutionalizes this act** by upholding that each person has a right to “informational self-determination”.
- **2016 - EU adopts General Data Protection Regulation (GDPR)** to modernize approach to data privacy
  - Enforceable as of 2018
  - “codified several key principles reflecting the Europeans' human-rights-based philosophical foundation for data privacy protection.”

General Data Protection Regulation (GDPR) is the model for emerging US state laws

The emerging US state laws are intended to be comprehensive in scope but are written to include carve-outs for data already protected under other laws (FERPA, HIPAA, etc).

Inside the New State Regulations

Philosophical Underpinnings of American Data Regulation

It could be said that American Data Regulation is a hodge-podge of different philosophical approaches that are somewhat reflective of the generations who instituted them. The American Revolution and its resulting Constitution established over time a philosophical blend of **Deontology** (principles, rights, duties that include duty to follow law) and **Libertarianism** (Bill of Rights that limit government power at the expense of individual rights and autonomy). The **Virtue Ethics** of the society during that time, including contemporary Christian moral virtues, were intended to provide the societal impetus to adhere to the responsibilities it contained. There are also elements of **egalitarian** philosophy (equal protection under the law) and **utilitarianism**. Modern legislation has become much more of a blend of **utilitarianism** and **egalitarianism**, but the coming data laws signal a desire to include more **deontological** and **libertarian** interventions.

American Data Regulations Philosophical Transition

- Shift from “harms-prevention-based” philosophy intended to mitigate harms in specific sectors found in preexisting federal laws
- A move toward a “rights-based” approach similar to the European Union's General Data Protection Regulation (GDPR)...” Historically this philosophy holds that data privacy is a fundamental human right. Individuals effectively own their personal information, and who can use it is a matter for them to decide.”

American Data Regulations Philosophical Transition

This shift from harms mitigation to a rights-based approach is incomplete.

- The move toward a rights-based approach is still filtered through domain compartmentalization
- some data is considered more sensitive than other data based on domain compartmentalization
- Inequitable application exists by nature due to the fact that people live in different states and interact with compartmentalized domains differently
- A federal negative liberty approach could unify and deepen all existing regulations and provide additional protections more in line with the Bill of Rights

Characteristics of the GDPR Mirrored in New American Regulations

- Governing Principles
- Establishes Formal Roles
- Establishes Specific Rights of Individuals

Characteristics of the GDPR Mirrored in New American Regulations – Governing Principles

- **Privacy or data protection by design** – data management systems should include privacy protections, data mapping, and account for data sensitivity.
- **Record-keeping** – the collection, processing, and use of data should be well-documented and readily producible.
- **Data minimization** – data containing personal information should be deleted after its use is completed.

Characteristics of the GDPR Mirrored in New American Regulations – Governing Principles

- **Transparency, informed consent, and legitimate uses** – easily-understandable informed consent is required for use, and then only for legally legitimate uses.
- **Data protection officers and data impact protection assessments** – Compliance with privacy protection requirements necessitates the use of trained professionals, and risk-management should be deployed for data protection assessments.
- **Best cybersecurity practices** – use cybersecurity best practices including physical and technological implements to minimize the risks of data breaches.

Characteristics of the GDPR Mirrored in New American Regulations – Governing Principles

- **Data breach notifications** – an incident response plan to deliver timely and appropriate notifications should be in place, tested, and meet deadlines according to law.
- **Employee training** – data policies should be rigorously designed and employees should be trained to perform those policies.
- **Requiring appropriate contractual language** – third party contracts should include provisions outlining adherence to relevant data regulations

Characteristics of the GDPR Mirrored in New American Regulations: Established Roles

Data controllers

entities who collect data

Data processors

those who decide what to do with data

Characteristics of the GDPR Mirrored in New American Regulations: Individual Rights for "Data Subjects"

Access

subjects have the right to request access to review their data

Correction

subjects have the right to request the correction of errors in their data

Portability

Subjects have the right to request the transfer of their data to another entity

Characteristics of the GDPR Mirrored in New American Regulations: Individual Rights for "Data Subjects"

Erasure

subjects have the right to request the deletion of their data

Consent

subjects have the right to decide on the sale of their data and its use in targeted advertising

Appeal

subjects have the right to appeal the denial of their request

New State Laws Based on the GDPR

- California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)
- Colorado Privacy Rights Act (CPA)
- Connecticut Data Privacy Act (CDPA)
- Utah Consumer Privacy Act (UCPA)
- Virginia Consumer Data Privacy Act (VCDPA)


California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)

- CCPA passed in 2018, CPRA went into effect Jan. 1, 2023
- Focused on Consumer Rights
- The only emerging state law that applies to Human Resources data
- Created a new state enforcement agency: the **California Privacy Protection Agency (CPPA)**

Colorado Privacy Rights Act (CPA)

- The Colorado Privacy Act (CPA) became effective on July 1, 2023.
- Requires data security and contract provisions for vendors and assessments for "high-risk" processing

Connecticut Data Privacy Act (CDPA)

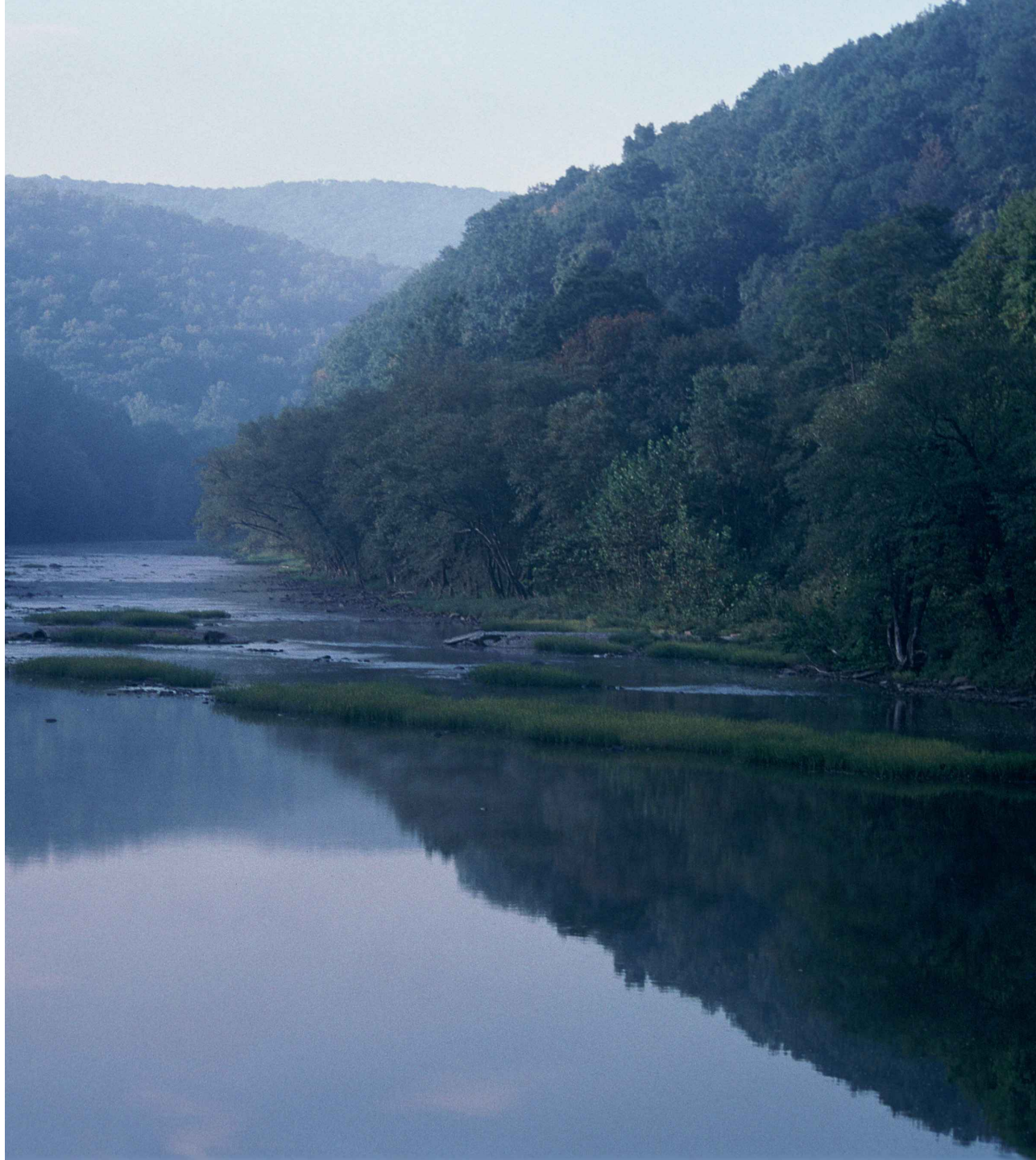
- In effect as of July 1, 2023
- Creates a suite of GDPR-like individual rights
- Requires data minimization, security, and assessments for "high risk" processing.

Utah Consumer Privacy Act (UCPA)

- Became effective on Dec. 31, 2023
- It provides for certain GDPR-like individual rights
- Requires data security and contract provisions
- Does not include expressly required risk assessments.

Virginia Consumer Data Privacy Act (VCDPA)

- Became effective Jan. 1, 2023
- Provides for certain GDPR-like individual rights, however in 2022, the "right-to-delete" was replaced with a right to opt out from certain processing



Tips to Guard Ourselves and Others

- Know the law. Don’t depend on someone else to know it for you. Ignorance of the law will not save you from prosecution. People throw others under the bus for their own mistakes all day everyday.
- Spend a good amount of time in your workplace’s policies and procedures manual and be able to reference relevant policies on command. Understand whether or not these policies and procedures meet the standards of applicable laws.
- If there are questions as to whether or not your workplace policies and procedures are lawful and compliant, make sure to ask your direct supervisor and document their answer. Memorialize it with an email to yourself.

Tips to Guard Ourselves and Others

- Start every project with a simple form that includes the project start date, the date of the query, the reason for the query, the intended work product, and the intended completion date.
- Log every action done to each working data set.
- Log every instance of sharing and by what avenue the data set is shared.
- Be able to produce your form and log on command. Create folders in your companies shared workspace for them and create a file nomenclature that is easy to follow and includes a date.

References

Black, Edwin. *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. Dialog Press, 2001.

Yale University International Toolkit. “Data Protection Laws” Yale University, 2024. www.world-toolkit.yale.edu/regulated-activity/data-protection-laws

Angwin, Julia. “You Know Who Else Collected Metadata? The Stasi.” ProPublica, 2014. www.propublica.org/article/how-the-stasi-spied-on-social-networks

Murray, Conor. “U.S. Data Privacy Protection Laws: A Comprehensive Guide.” Forbes, April 25, 2023. www.forbes.com/sites/conormurray/2023/04/21/us-data-privacy-protection-laws-a-comprehensive-guide/?sh=7f76a0c25f92

Harrington, David. “A Step-By-Step Guide to California Consumer Privacy Act (CCPA) Compliance.” Varonis, May 9, 2023. www.varonis.com/blog/ccpa-compliance

Californial Privacy Protection Agency. “Laws & Regulations”. State of California, 2024. cppa.ca.gov/regulations/

Ben-Hassine, Wafa. “Government Internet Policy Must be Rights-Based and User Centered”. UN Chronicle. www.un.org/en/chronicle/article/government-policy-internet-must-be-rights-based-and-user-centred

Bellamy, Frederic D. “U.S. data privacy laws to enter new era in 2023” Reuters, 2023. www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/

University of Michigan IT Services Safe Computing. “History of Privacy Timeline”. www.safecomputing.umich.edu/protect-privacy/history-of-privacy-timeline

United States Department of Education. “Data Literacy” October, 2021. www.ed.gov/sites/default/files/documents/stem/20211015-data-literacy.pdf

McNamee, Roger. “Opinion: The misuse of personal data is everywhere. Here’s one measure that fights back ” Los Angeles Times, September, 2023. www.latimes.com/opinion/story/2023-09-06/personal-data-privacy-delete-act-california-sb-362