6 April 2023

Data Protection & Computer Crime Law

Sunoo Park
Postdoctoral Fellow, **Columbia University**
Visiting Fellow, **Columbia Law School**

Computer Security II (COMS W4182, Spring 2023) | **Guest Lecture**

Data protection law

Governs legal obligations of entities that obtain, process, and store specific kinds of (personal) data.

Data protection law

Governs legal obligations of entities that obtain, process, and store specific kinds of (personal) data.

Computer crime law

Defines **crimes** related to the use of computers.

Data protection law

Governs legal obligations of entities that obtain, process, and store specific kinds of (personal) data.

Computer crime law

Defines **crimes** related to the use of computers.

Data protection law

Governs legal obligations of entities that obtain, process, and store specific kinds of (personal) data.

Computer crime law

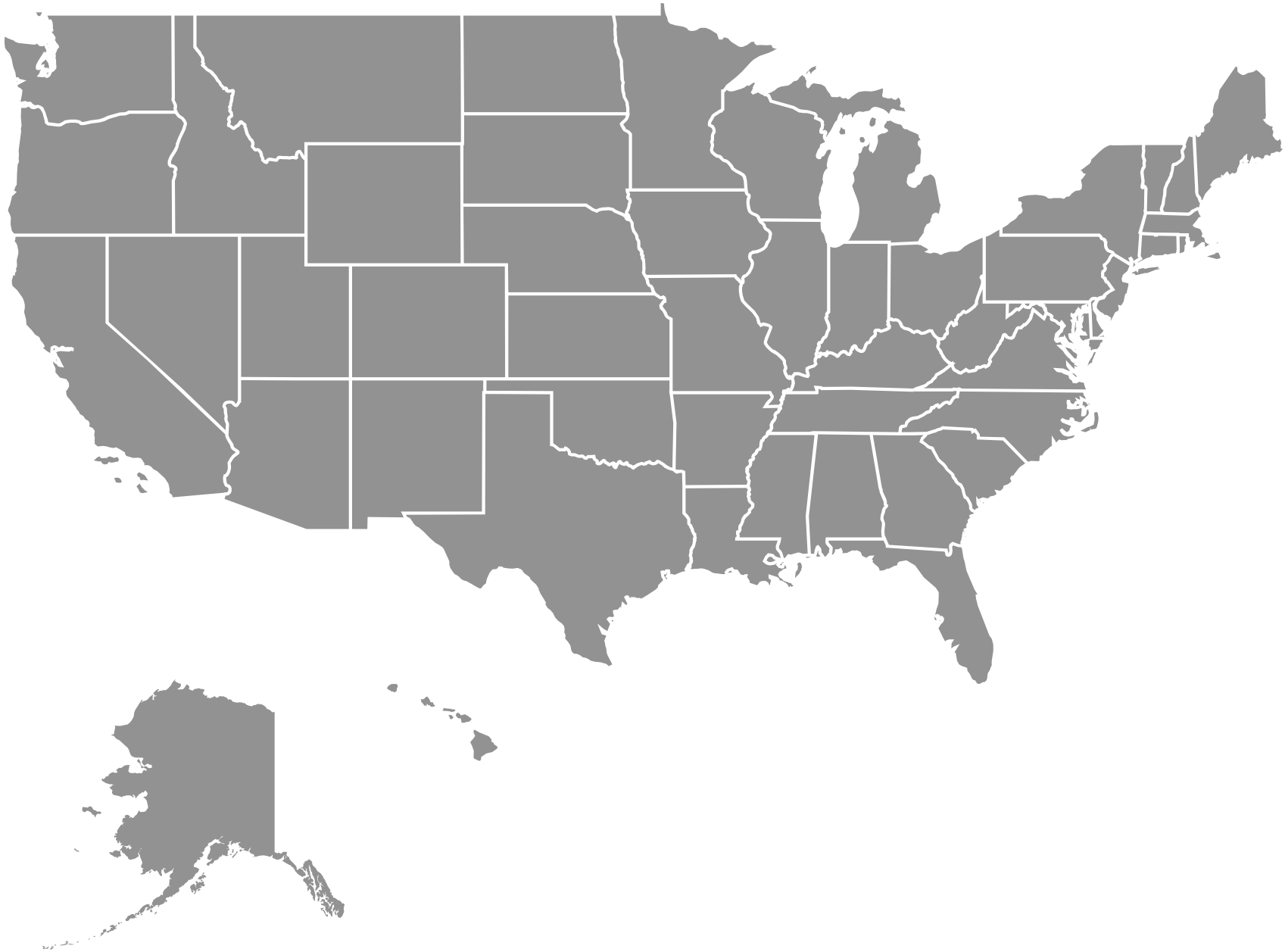
Defines **crimes** related to the use of computers.

Crime

Conduct that is defined by law as
punishable by incarceration or other penalties.

1. Data protection law

U.S. federal and state law



Federal data protection laws

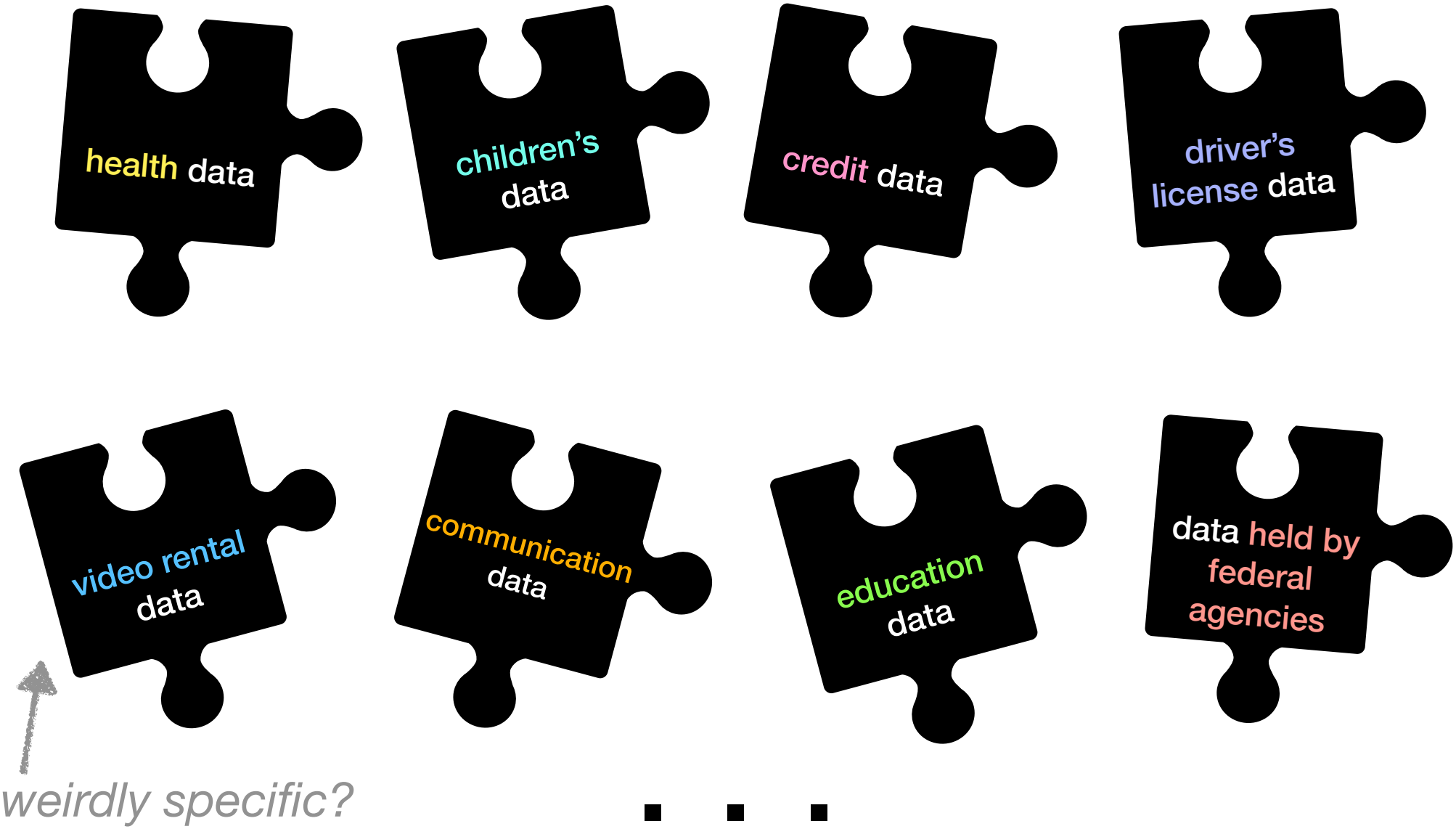
A patchwork of sector-specific laws

Federal data protection laws

A patchwork of sector-specific laws

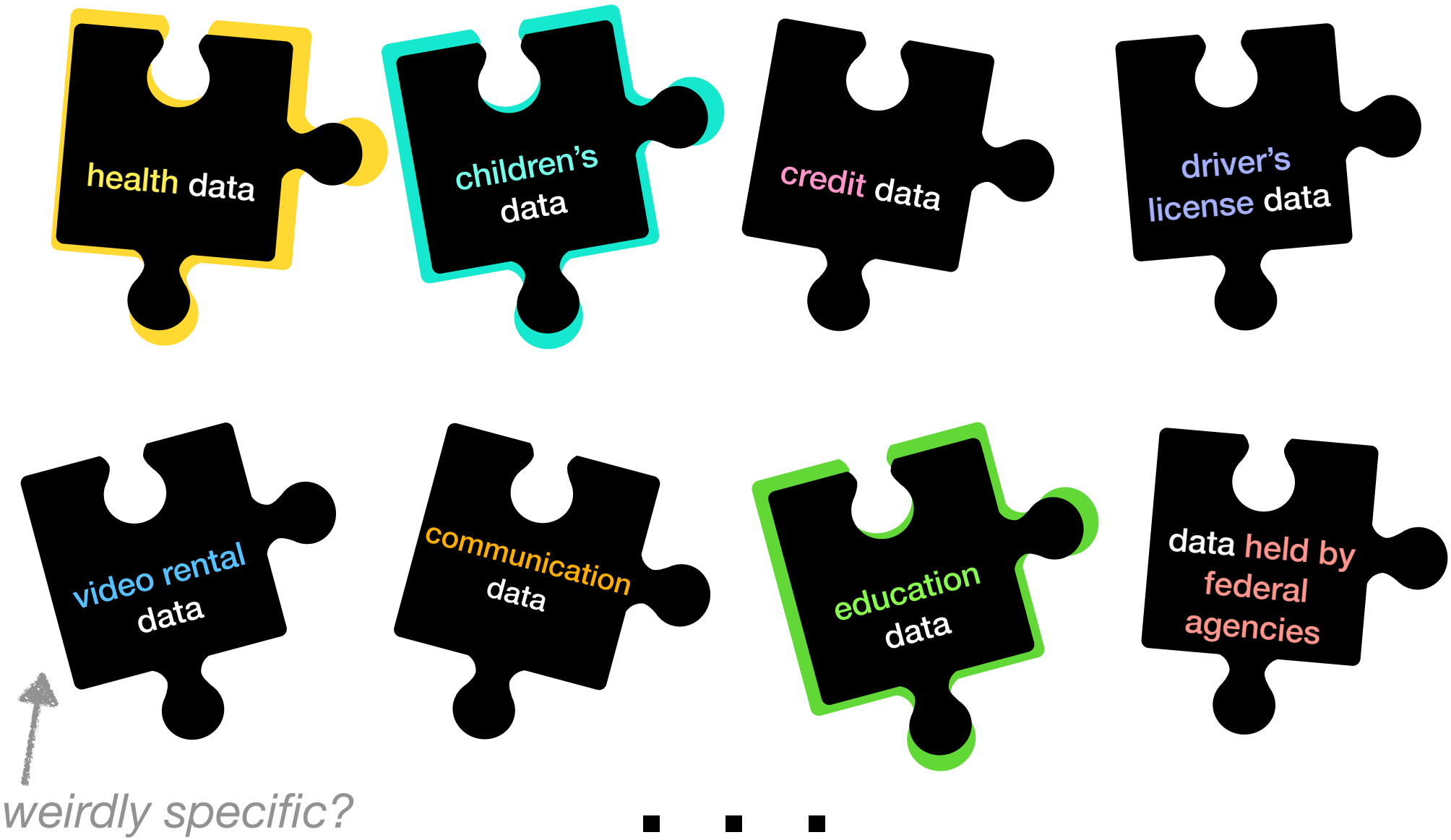
Federal data protection laws

A patchwork of sector-specific laws



Federal data protection laws

A patchwork of sector-specific laws



Are you
“protecting privacy”
if you comply with
data protection laws?

Are you **adequately**
“protecting privacy”
if you comply with
data protection laws?


health data

Health Insurance Portability & Accountability Act ("HIPAA")

Health Insurance Portability & Accountability Act ("HIPAA")

- **Entities:** Applies to **health care providers**, **health plans**, **health care clearinghouses**, and some of their **business associates**.

Health Insurance Portability & Accountability Act ("HIPAA")

- **Entities:** Applies to **health care providers**, **health plans**, **health care clearinghouses**, and some of their **business associates**.
  - Not any health-related app!

Health Insurance Portability & Accountability Act ("HIPAA")

- **Entities:** Applies to **health care providers**, **health plans**, **health care clearinghouses**, and some of their **business associates**.
  - Not any health-related app!
- **Data:** Applies to protected health information (PHI), meaning "individually identifiable health information," i.e., data related to

Health Insurance Portability & Accountability Act ("HIPAA")

- **Entities:** Applies to **health care providers**, **health plans**, **health care clearinghouses**, and some of their **business associates**.
  - Not any health-related app!
- **Data:** Applies to protected health information (PHI), meaning "individually identifiable health information," i.e., data related to
  - an individual's past/present/future physical or mental health,

Health Insurance Portability & Accountability Act ("HIPAA")

- **Entities:** Applies to **health care providers**, **health plans**, **health care clearinghouses**, and some of their **business associates**.
  - Not any health-related app!
- **Data:** Applies to protected health information (PHI), meaning "individually identifiable health information," i.e., data related to
  - an individual's past/present/future physical or mental health,
  - the provision of health care to the individual,

Health Insurance Portability & Accountability Act ("HIPAA")

- **Entities:** Applies to **health care providers**, **health plans**, **health care clearinghouses**, and some of their **business associates**.
  - Not any health-related app!
- **Data:** Applies to protected health information (PHI), meaning "individually identifiable health information," i.e., data related to
  - an individual's past/present/future physical or mental health,
  - the provision of health care to the individual,
  - the past/present/future payment for the provision of health care to the individual.

YOUR DATA AND PRIVACY

Health apps share your concerns with advertisers. HIPAA can't stop it.

From 'depression' to 'HIV,' we found popular health apps sharing potential health concerns and user identifiers with dozens of ad companies

By Tatum Hunter and Jeremy B. Merrill

Updated September 22, 2022 at 10:26 a.m. EDT | Published September 22, 2022 at 7:00 a.m. EDT

Health Insurance Portability & Accountability Act ("HIPAA")

- **De-identified health information** is not covered.
  - What's considered de-identified?
    - Formal determination by a qualified statistician, or
    - Removal of specified identifiers of the individual (and relatives, household members, and employers), and the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

Privacy

Researchers spotlight the lie of 'anonymous' data

Natasha Lomas @riptari / 6:30 AM EDT • July 24, 2019

Comment

Image Credits: blvdone / Shutterstock

Researchers from two universities in Europe have published a method they say is able to correctly re-identify 99.98% of individuals in anonymized data sets with just 15 demographic attributes.

Their model suggests complex data sets of personal information cannot be protected against re-identification by current methods of "anonymizing" data — such as releasing samples (subsets) of the information.

Indeed, the suggestion is that no "anonymized" and released big data set can be considered safe from re-identification — not without strict access controls.

Health Insurance Portability & Accountability Act ("HIPAA")

Health Insurance Portability & Accountability Act (“HIPAA”)

- Covered entities may not use or disclosure PHI except (1) as required or permitted by the HIPAA Privacy Rule or (2) with written authorization from the person who is the subject of the information.

Health Insurance Portability & Accountability Act ("HIPAA")

- Covered entities may not use or disclosure PHI except (1) as required or permitted by the HIPAA Privacy Rule or (2) with written authorization from the person who is the subject of the information.
- **Required disclosures:** A covered entity **must** disclose PHI:
  - To individuals (or their representatives) when they request
    - access to their PHI, or
    - an accounting of disclosures of their PHI by the covered entity.
  - To the US Dept of Health & Human Services (HHS) when HHS is undertaking an investigation or other procedure.

Health Insurance Portability & Accountability Act ("HIPAA")

- Covered entities may not use or disclosure PHI except (1) as required or permitted by the HIPAA Privacy Rule or (2) with written authorization from the person who is the subject of the information.
- **Required disclosures:** A covered entity **must** disclose PHI:
  - To individuals (or their representatives) when they request
    - access to their PHI, or
    - an accounting of disclosures of their PHI by the covered entity.
  - To the US Dept of Health & Human Services (HHS) when HHS is undertaking an investigation or other procedure.
- **Permitted disclosures:**
  - To the person who is the subject of the information.
  - For treatment, payment, and health care operations.
  - For specific public-interest activities.


children's data

Children's Online Privacy Protection Rule ("COPPA")

Children's Online Privacy Protection Rule ("COPPA")

- **Entities:** Applies to:
  - operators of websites/online services directed to children under 13 years of age, and
  - operators of other websites/online services that have actual knowledge that they are collecting **personal information** online from a child under 13 years of age.

Children's Online Privacy Protection Rule ("COPPA")

- **Entities:** Applies to:
  - operators of websites/online services directed to children under 13 years of age, and
  - operators of other websites/online services that have actual knowledge that they are collecting **personal information** online from a child under 13 years of age.
- **Data:** **Personal information** means:
  - Name, physical address (or geolocation info), online contact info, usernames, phone #, SSN, photo/video/audio files containing a child's image or voice.
  - Any other info about the child (or parents) that the operator collects online from the child and combines w/ any of the above.

Children's Online Privacy Protection Rule ("COPPA")

Children's Online Privacy Protection Rule ("COPPA")

- **Covered operators must:**

Children's Online Privacy Protection Rule ("COPPA")

- **Covered operators must:**
  1. Post a clear & comprehensive online **privacy policy**…

Children's Online Privacy Protection Rule ("COPPA")

- **Covered operators must:**
  1. Post a clear & comprehensive online **privacy policy**…
  2. Obtain **verifiable parental consent before** collecting personal info online from children (with limited exceptions).

Children's Online Privacy Protection Rule ("COPPA")

- **Covered operators must:**
  1. Post a clear & comprehensive online **privacy policy**…
  2. Obtain **verifiable parental consent before** collecting personal info online from children (with limited exceptions).
  3. Give parents the option to **consent only to the operator**'s collection and internal use of a child's information…

Children's Online Privacy Protection Rule ("COPPA")

- **Covered operators must:**
  1. Post a clear & comprehensive online **privacy policy**…
  2. Obtain **verifiable parental consent before** collecting personal info online from children (with limited exceptions).
  3. Give parents the option to **consent only to the operator**'s collection and internal use of a child's information…
  4. Allow parents **access** to their child's personal information to review and allow parents to **have the information deleted**.

Children's Online Privacy Protection Rule ("COPPA")

- **Covered operators must:**
  1. Post a clear & comprehensive online **privacy policy**…
  2. Obtain **verifiable parental consent before** collecting personal info online from children (with limited exceptions).
  3. Give parents the option to **consent only to the operator**'s collection and internal use of a child's information…
  4. Allow parents **access** to their child's personal information to review and allow parents to **have the information deleted**.
  5. Allow parents to **prevent further use/collection** of a child's personal info.

Children's Online Privacy Protection Rule ("COPPA")

- **Covered operators must:**
  1. Post a clear & comprehensive online **privacy policy**…
  2. Obtain **verifiable parental consent before** collecting personal info online from children (with limited exceptions).
  3. Give parents the option to **consent only to the operator**'s collection and internal use of a child's information…
  4. Allow parents **access** to their child's personal information to review and allow parents to **have the information deleted**.
  5. Allow parents to **prevent further use/collection** of a child's personal info.
  6. **Maintain confidentiality, security, & integrity** of information collected from children, including reasonable access control.

Children's Online Privacy Protection Rule ("COPPA")

- **Covered operators must:**
  1. Post a clear & comprehensive online **privacy policy**…
  2. Obtain **verifiable parental consent before** collecting personal info online from children (with limited exceptions).
  3. Give parents the option to **consent only to the operator**'s collection and internal use of a child's information…
  4. Allow parents **access** to their child's personal information to review and allow parents to **have the information deleted**.
  5. Allow parents to **prevent further use/collection** of a child's personal info.
  6. **Maintain confidentiality, security, & integrity** of information collected from children, including reasonable access control.
  7. **Retain children's info for only as long as necessary** to fulfill the purpose for which it was collected; delete with **reasonable deletion procedures**.

Children's Online Privacy Protection Rule ("COPPA")

- **Covered operators must:**
  1. Post a clear & comprehensive online **privacy policy**…
  2. Obtain **verifiable parental consent before** collecting personal info online from children (with limited exceptions).
  3. Give parents the option to **consent only to the operator**'s collection and internal use of a child's information…
  4. Allow parents **access** to their child's personal information to review and allow parents to **have the information deleted**.
  5. Allow parents to **prevent further use/collection** of a child's personal info.
  6. **Maintain confidentiality, security, & integrity** of information collected from children, including reasonable access control.
  7. **Retain children's info for only as long as necessary** to fulfill the purpose for which it was collected; delete with **reasonable deletion procedures**.
  8. **Not condition a child's participation in an online activity** on the child providing more information than is reasonably necessary to participate.

(Sean Loose/Illustration for The Washington Post)

WE THE USERS

Your kids' apps are spying on them

Apple and Google just look the other way. Here's how we stop it.

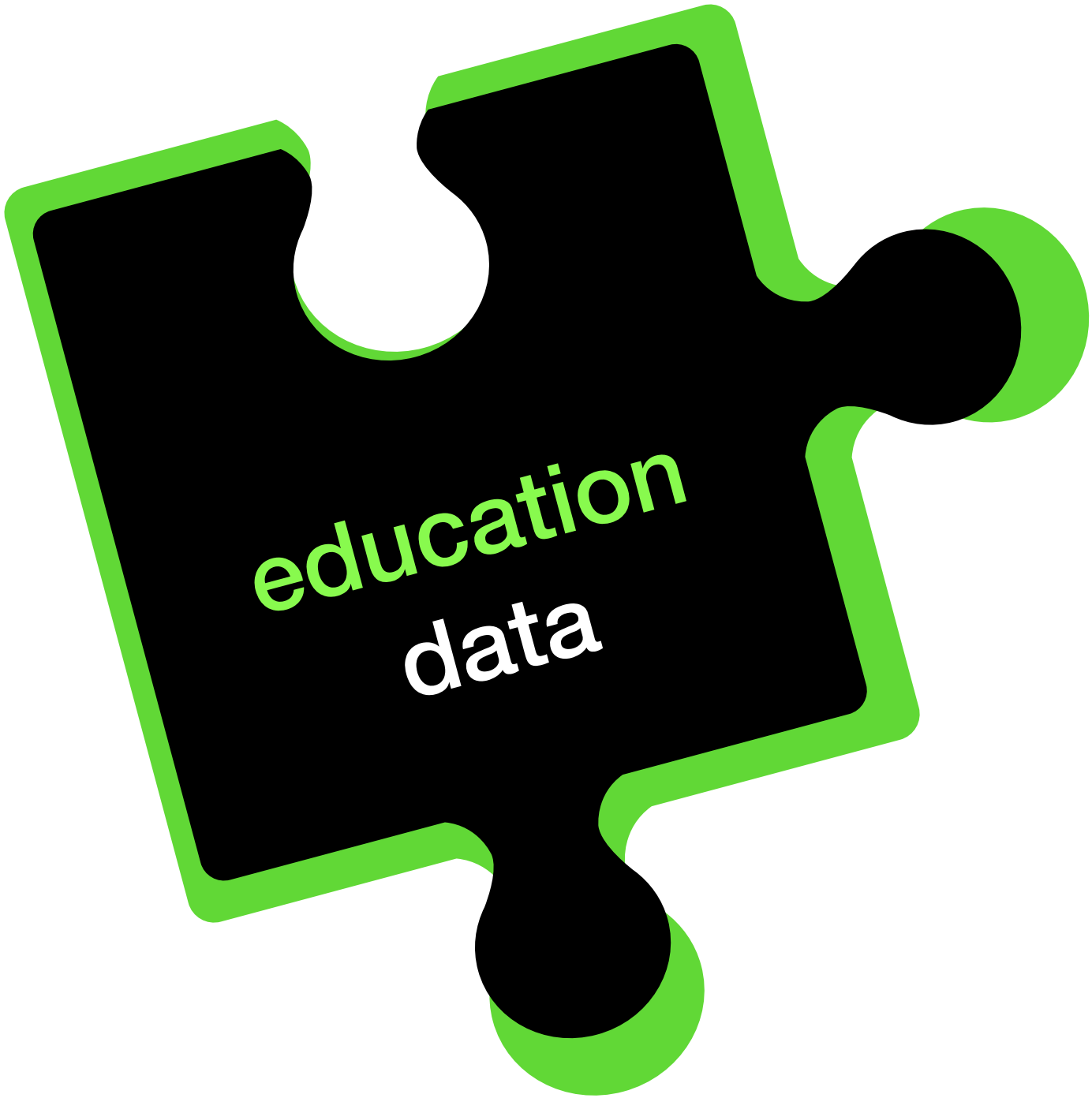
By Geoffrey A. Fowler

June 9, 2022 at 8:00 a.m. EDT

Imagine if a stranger parked in front of a child's bedroom window to peep inside. You'd call the police.

Yet that happens every day online, and Big Tech looks the other way.

Apps are spying on our kids at a scale that should shock you. More than two-thirds of the 1,000 most popular iPhone apps likely to be used by children collect and send their personal information out to the advertising industry, according to a major new study shared with me by fraud and compliance software company Pixalate. On Android, 79 percent of popular kids apps do the same.


education
data

Family Educational Rights & Privacy Act (“FERPA”)

Family Educational Rights & Privacy Act (“FERPA”)

- **Entities:** Most elementary schools, secondary schools, post-secondary schools. Also any state/local agency that receives federal Dept of Education funds.

Family Educational Rights & Privacy Act (“FERPA”)

- **Entities:** Most elementary schools, secondary schools, post-secondary schools. Also any state/local agency that receives federal Dept of Education funds.
- **Data:** (**Personally identifiable info** in) **education records**.

Family Educational Rights & Privacy Act (“FERPA”)

- **Entities:** Most elementary schools, secondary schools, post-secondary schools. Also any state/local agency that receives federal Dept of Education funds.
- **Data:** (**Personally identifiable info** in) **education records**.
- **Primary purposes:**

Family Educational Rights & Privacy Act (“FERPA”)

- **Entities:** Most elementary schools, secondary schools, post-secondary schools. Also any state/local agency that receives federal Dept of Education funds.
- **Data:** (**Personally identifiable info** in) **education records**.
- **Primary purposes:**
    1. Give **parents** / **eligible students** more control over their educational records.

Family Educational Rights & Privacy Act (“FERPA”)

- **Entities:** Most elementary schools, secondary schools, post-secondary schools. Also any state/local agency that receives federal Dept of Education funds.
- **Data:** (**Personally identifiable info** in) **education records**.
- **Primary purposes:**
  1. Give **parents** / **eligible students** more control over their educational records.
  2. Prohibit institutions from disclosing PII in education records without consent of **parents** / **eligible students**.

Family Educational Rights & Privacy Act (“FERPA”)

- **Entities:** Most elementary schools, secondary schools, post-secondary schools. Also any state/local agency that receives federal Dept of Education funds.
- **Data:** (**Personally identifiable info** in) **education records**.
- **Primary purposes:**
  1. Give **parents** / **eligible students** more control over their educational records.
  2. Prohibit institutions from disclosing PII in education records without consent of **parents** / **eligible students**.
- **Eligible student**: ≥ 18 or attends a school above high school level.

Family Educational Rights & Privacy Act ("FERPA")

- **Entities:** Most elementary schools, secondary schools, post-secondary schools. Also any state/local agency that receives federal Dept of Education funds.
- **Data:** (**Personally identifiable info** in) **education records**.
- **Primary purposes:**
  1. Give **parents** / **eligible students** more control over their educational records.
  2. Prohibit institutions from disclosing PII in education records without consent of **parents** / **eligible students**.
- **Eligible student**: ≥ 18 or attends a school above high school level.
- **Education record**: (1) directly related to a student and (2) maintained by an educational institution or by a party acting for the institution.

Family Educational Rights & Privacy Act (“FERPA”)

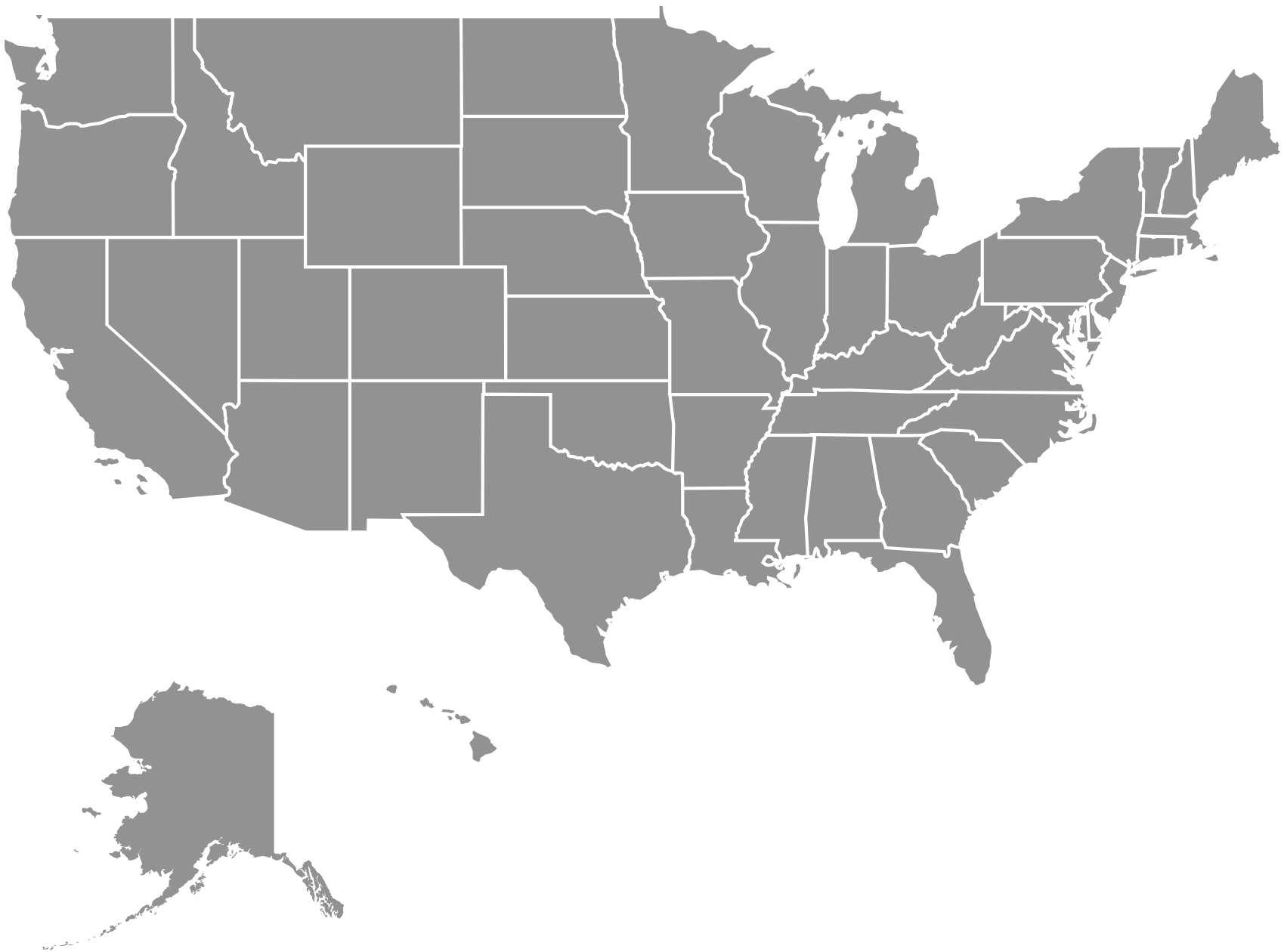
Family Educational Rights & Privacy Act ("FERPA")

- **Rights of parents / eligible students:**
  - To **inspect the student's education records** kept by the school.
  - To **request correction** of records that they believe are **incorrect** or **misleading**.
    - If the school refuses, the parent / eligible student has a right to a **formal hearing**.
    - After the hearing, if the school still does not change the record, the parent / eligible student has a right to file a **statement explaining their view**, alongside the record.
  - To **stop the release of PII**.
  - To have a **copy of the institution's policy** concerning access to educational records.

Family Educational Rights & Privacy Act ("FERPA")

- **<u>Institutions may not disclose PII without consent, except:</u>**
  - To school officials with a legitimate educational interest.
  - Other schools to which a student is transferring.
  - Certain officials for evaluation/audit purposes.
  - Certain parties wrt financial aid for the student.
  - Organizations conducting certain studies for the school.
  - Accrediting organizations.
  - Certain officials in health/safety emergencies.
  - State/local authorities within a juvenile justice system.
  - To comply with a judicial order or lawful subpoena.

Okay, but
what does this have to do
with **computers**?



Illinois Biometric Information Privacy Act ("BIPA")

- The first state biometric privacy law, passed in 2008.
- Prohibits private companies from collecting biometric data unless they:
  - inform the person in writing of **what data is collected/stored**,
  - inform the person in writing of the **specific purposes** and **length of time** for which the data will be used,
  - obtain the person's **written consent**.

State data protection laws

Security breach laws

State data protection laws

Security breach laws

- All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have **security breach notification laws** that require businesses or governments to notify consumers or citizens if their personal information is breached.

State data protection laws

Security breach laws

- All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have **security breach notification laws** that require businesses or governments to notify consumers or citizens if their personal information is breached.
- At least 19 states introduced or considered measures in 2022 that would amend existing security breach laws.

State data protection laws

Security breach laws

- All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have **security breach notification laws** that require businesses or governments to notify consumers or citizens if their personal information is breached.
- At least 19 states introduced or considered measures in 2022 that would amend existing security breach laws.
- Trends:

State data protection laws

Security breach laws

- All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have **security breach notification laws** that require businesses or governments to notify consumers or citizens if their personal information is breached.
- At least 19 states introduced or considered measures in 2022 that would amend existing security breach laws.
- Trends:
  - Establish/shorten time frame to report breach.

State data protection laws

Security breach laws

- All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have **security breach notification laws** that require businesses or governments to notify consumers or citizens if their personal information is breached.
- At least 19 states introduced or considered measures in 2022 that would amend existing security breach laws.
- Trends:
  - Establish/shorten time frame to report breach.
  - Require state/local govt entities to report breaches.

State data protection laws

Security breach laws

- All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have **security breach notification laws** that require businesses or governments to notify consumers or citizens if their personal information is breached.
- At least 19 states introduced or considered measures in 2022 that would amend existing security breach laws.
- Trends:
  - Establish/shorten time frame to report breach.
  - Require state/local govt entities to report breaches.
  - Protections for entities that had reasonable security practices in place at the time of a breach.

State data protection laws

Security breach laws

- All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have **security breach notification laws** that require businesses or governments to notify consumers or citizens if their personal information is breached.
- At least 19 states introduced or considered measures in 2022 that would amend existing security breach laws.
- Trends:
  - Establish/shorten time frame to report breach.
  - Require state/local govt entities to report breaches.
  - Protections for entities that had reasonable security practices in place at the time of a breach.
  - Expand definitions of personal information to include biometric/health/etc.

DO DATA BREACH NOTIFICATION LAWS WORK?

Aniket Kesari [*]

Over 2.8 million Americans have reported being victims identify theft in recent years, costing the U.S. economy at least $13 billion in 2020. In response to this growing problem, all 50 states have enacted some form of data breach notification law in the past 20 years. Despite their prevalence, evaluating the efficacy of these laws remains elusive. This Article fills this gap, while further creating a new taxonomy to understand when these laws work and when they do not.

Legal scholars have generally treated data breach notification laws as doing just one thing—disclosing information to consumers. But this approach ignores rich variation: differences in disclosure requirements to regulators and credit monitoring agencies; varied mechanisms for public and private enforcement; and a range of thresholds that define how firms should assess the likelihood that a data breach will ultimately harm consumers.

This Article leverages the Federal Trade Commission's Consumer Sentinel database to build a comprehensive dataset measuring identity theft report rates since 2000. Using staggered adoption synthetic control – a popular method for policy evaluation that has yet to be widely applied in empirical legal studies – this Article finds that whether identify theft laws work depends on which of these different strands of legal provisions are employed. In particular, while baseline disclosure requirements and private rights of action have small effects, requiring firms to notify state regulators reduces identity theft report rates by approximately 10%. And surprisingly, laws that fail to exclude low-risk breaches from reporting requirements are counterproductive, increasing identify theft report rates by 4%.

The Article ties together these results within a functional typology: namely, whether legal provisions (1) enable consumer mitigation of data breach harms, or (2) encourage organizations to invest in better data security. It explains how these results and typology provide lessons for current federal and state proposals to expand or amend the scope of breach notification laws. A new federal law that simply mimics existing baseline

---

[*] Research Fellow, Information Law Institute, New York University. I thank Elliott Ash, Stefan Bechtold, Elettra Bietti, Kat Geddes, Amit Haim, James Hicks, Chris Hoofnagle, Jiaying Jiang, Christine Jolls, Sonia Katyal, Filippo Lancieri, Lawrence Liu, Tejas

DO DATA BREACH NOTIFICATION LAWS WORK?

Aniket Kesari [*]

Over 2.8 million Americans have reported being victims identify theft in recent years, costing the U.S. economy at least $13 billion in 2020. In response to this growing problem, all 50 states have enacted some form of data breach notification law in the past 20 years. Despite their prevalence, evaluating the efficacy of these laws remains elusive. This Article fills this gap, while further creating a new taxonomy to understand when these laws work and when they do not.

Legal scholars have generally treated data breach notification laws as doing just one thing—disclosing information to consumers. But this approach ignores rich variation: differences in disclosure requirements to regulators and credit monitoring agencies; varied mechanisms for public and private enforcement; and a range of thresholds that define how firms should assess the likelihood that a data breach will ultimately harm consumers.

This Article leverages the Federal Trade Commission's Consumer Sentinel database to build a comprehensive dataset measuring identity theft report rates since 2000. Using staggered adoption synthetic control – a popular method for policy evaluation that has yet to be widely applied in empirical legal studies – this Article finds that whether identify theft laws work depends on which of these different strands of legal provisions are employed. In particular, while baseline disclosure requirements and private rights of action have small effects, requiring firms to notify state regulators reduces identity theft report rates by approximately 10%. And surprisingly, laws that fail to exclude low-risk breaches from reporting requirements are counterproductive, increasing identify theft report rates by 4%.

The Article ties together these results within a functional typology: namely, whether legal provisions (1) enable consumer mitigation of data breach harms, or (2) encourage organizations to invest in better data security. It explains how these results and typology provide lessons for current federal and state proposals to expand or amend the scope of breach notification laws. A new federal law that simply mimics existing baseline

---

[*] Research Fellow, Information Law Institute, New York University. I thank Elliott Ash, Stefan Bechtold, Elettra Bietti, Kat Geddes, Amit Haim, James Hicks, Chris Hoofnagle, Jiaying Jiang, Christine Jolls, Sonia Katyal, Filippo Lancieri, Lawrence Liu, Tejas

DO DATA BREACH NOTIFICATION LAWS WORK?

Aniket Kesari [*]

Over 2.8 million Americans have reported being victims identify theft in recent years, costing the U.S. economy at least $13 billion in 2020. In response to this growing problem, all 50 states have enacted some form of data breach notification law in the past 20 years. Despite their prevalence, evaluating the efficacy of these laws remains elusive. This Article fills this gap, while further creating a new taxonomy to understand when these laws work and when they do not.

Legal scholars have generally treated data breach notification laws as doing just one thing—disclosing information to consumers. But this approach ignores rich variation: differences in disclosure requirements to regulators and credit monitoring agencies; varied mechanisms for public and private enforcement; and a range of thresholds that define how firms should assess the likelihood that a data breach will ultimately harm consumers.

This Article leverages the Federal Trade Commission's Consumer Sentinel database to build a comprehensive dataset measuring identity theft report rates since 2000. Using staggered adoption synthetic control – a popular method for policy evaluation that has yet to be widely applied in empirical legal studies – this Article finds that whether identify theft laws work depends on which of these different strands of legal provisions are employed. In particular, while baseline disclosure requirements and private rights of action have small effects, requiring firms to notify state regulators reduces identity theft report rates by approximately 10%. And surprisingly, laws that fail to exclude low-risk breaches from reporting requirements are counterproductive, increasing identify theft report rates by 4%.

The Article ties together these results within a functional typology: namely, whether legal provisions (1) enable consumer mitigation of data breach harms, or (2) encourage organizations to invest in better data security. It explains how these results and typology provide lessons for current federal and state proposals to expand or amend the scope of breach notification laws. A new federal law that simply mimics existing baseline

---

[*] Research Fellow, Information Law Institute, New York University. I thank Elliott Ash, Stefan Bechtold, Elettra Bietti, Kat Geddes, Amit Haim, James Hicks, Chris Hoofnagle, Jiaying Jiang, Christine Jolls, Sonia Katyal, Filippo Lancieri, Lawrence Liu, Tejas

Looking beyond the US…

The EU Approach

The General Data Protection Regulation (GDPR)

The EU Approach

The General Data Protection Regulation (GDPR)

- Passed in 2016, came into effect 2018.
- Two main objectives:
  - Protect “fundamental rights and freedoms of natural persons” regarding **protection of their personal data**.
  - Consolidate differing EU member state laws and ensure the “**free movement of personal data** within the Union.”
- Large fines: up to max{20M euros, 4% of global annual income}
- Implemented by authorities in each EU member country.

The EU Approach

The General Data Protection Regulation (GDPR)

The EU Approach

The General Data Protection Regulation (GDPR)

- **Entities:** Any entity that **processes** personal data (wholly/partly by automated means, or as part of a filing system).

The EU Approach

The General Data Protection Regulation (GDPR)

- **Entities:** Any entity that **processes** personal data (wholly/partly by automated means, or as part of a filing system).
  - With offices/personnel in Europe, or

The EU Approach

The General Data Protection Regulation (GDPR)

- **Entities:** Any entity that **processes** personal data (wholly/partly by automated means, or as part of a filing system).
  - With offices/personnel in Europe, or
  - Offering goods/services (even if free) to people in Europe.

The EU Approach

The General Data Protection Regulation (GDPR)

- **Entities:** Any entity that **processes** personal data (wholly/partly by automated means, or as part of a filing system).
  - With offices/personnel in Europe, or
  - Offering goods/services (even if free) to people in Europe.
- **Personal data**: any information relating to an identified or identifiable natural person ('**data subject**'); an **identifiable natural person** is one who can be identified, directly or indirectly…

The EU Approach

The General Data Protection Regulation (GDPR)

- **Entities:** Any entity that **processes** personal data (wholly/partly by automated means, or as part of a filing system).
  - With offices/personnel in Europe, or
  - Offering goods/services (even if free) to people in Europe.
- **Personal data**: any information relating to an identified or identifiable natural person ('**data subject**'); an **identifiable natural person** is one who can be identified, directly or indirectly…
- **Processing**: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, … destruction.

The EU Approach

The General Data Protection Regulation (GDPR)

The EU Approach

The General Data Protection Regulation (GDPR)

- **Legal bases for processing:**
  1. **Consent** of data subject

The EU Approach

The General Data Protection Regulation (GDPR)

- **Legal bases for processing:**
  1. **Consent** of data subject
  2. Necessary to **perform a contract** that the data subject has agreed to (or requested)

The EU Approach

The General Data Protection Regulation (GDPR)

- **Legal bases for processing:**
  1. **Consent** of data subject
  2. Necessary to **perform a contract** that the data subject has agreed to (or requested)
  3. Necessary for **compliance with a legal obligation**

The EU Approach

The General Data Protection Regulation (GDPR)

- **Legal bases for processing:**
  1. **Consent** of data subject
  2. Necessary to **perform a contract** that the data subject has agreed to (or requested)
  3. Necessary for **compliance with a legal obligation**
  4. Necessary to protect **vital interests** of data subject or another natural person

The EU Approach

The General Data Protection Regulation (GDPR)

- **Legal bases for processing:**
  1. **Consent** of data subject
  2. Necessary to **perform a contract** that the data subject has agreed to (or requested)
  3. Necessary for **compliance with a legal obligation**
  4. Necessary to protect **vital interests** of data subject or another natural person
  5. Necessary for the exercise of **official authority** or for certain **public interest** activities

The EU Approach

The General Data Protection Regulation (GDPR)

- **Legal bases for processing:**
  1. **Consent** of data subject
  2. Necessary to **perform a contract** that the data subject has agreed to (or requested)
  3. Necessary for **compliance with a legal obligation**
  4. Necessary to protect **vital interests** of data subject or another natural person
  5. Necessary for the exercise of **official authority** or for certain **public interest** activities
  6. Necessary for **legitimate interests** of processor that do not outweigh the privacy interests of data subjects

The EU Approach

The General Data Protection Regulation (GDPR)

- **Legal bases for processing:**
  1. **Consent** of data subject
  2. Necessary to **perform a contract** that the data subject has agreed to (or requested)
  3. Necessary for **compliance with a legal obligation**
  4. Necessary to protect **vital interests** of data subject or another natural person
  5. Necessary for the exercise of **official authority** or for certain **public interest** activities
  6. Necessary for **legitimate interests** of processor that do not outweigh the privacy interests of data subjects
     - E.g., to secure data, prevent fraud, or offer better service.

The EU Approach

The General Data Protection Regulation (GDPR)

The EU Approach

The General Data Protection Regulation (GDPR)

- **Rights of data subjects:**
  1. **Transparent info** & comms to exercise data rights

The EU Approach

The General Data Protection Regulation (GDPR)

- **Rights of data subjects:**
  1. **Transparent info** & comms to exercise data rights
  2. Right of **access**

The EU Approach

The General Data Protection Regulation (GDPR)

- **Rights of data subjects:**
  1. **Transparent info** & comms to exercise data rights
  2. Right of **access**
  3. Right to **rectification**

The EU Approach

The General Data Protection Regulation (GDPR)

- **Rights of data subjects:**
  1. **Transparent info** & comms to exercise data rights
  2. Right of **access**
  3. Right to **rectification**
  4. Right to **erasure**

The EU Approach

The General Data Protection Regulation (GDPR)

- **Rights of data subjects:**
  1. **Transparent info** & comms to exercise data rights
  2. Right of **access**
  3. Right to **rectification**
  4. Right to **erasure**
  5. Right to **restriction of processing**

The EU Approach

The General Data Protection Regulation (GDPR)

- **Rights of data subjects:**
  1. **Transparent info** & comms to exercise data rights
  2. Right of **access**
  3. Right to **rectification**
  4. Right to **erasure**
  5. Right to **restriction of processing**
  6. Right to **notification**

The EU Approach

The General Data Protection Regulation (GDPR)

- **Rights of data subjects:**
  1. **Transparent info** & comms to exercise data rights
  2. Right of **access**
  3. Right to **rectification**
  4. Right to **erasure**
  5. Right to **restriction of processing**
  6. Right to **notification**
  7. Right to **data portability**

The EU Approach

The General Data Protection Regulation (GDPR)

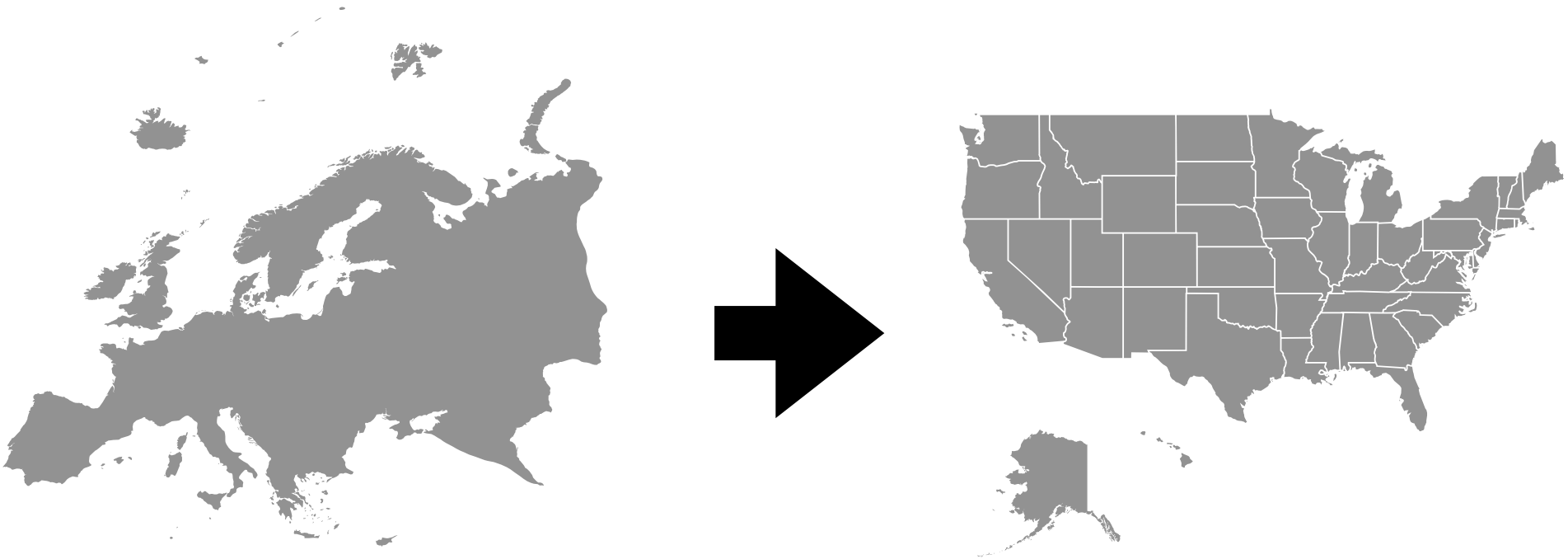
- **Rights of data subjects:**
  1. **Transparent info** & comms to exercise data rights
  2. Right of **access**
  3. Right to **rectification**
  4. Right to **erasure**
  5. Right to **restriction of processing**
  6. Right to **notification**
  7. Right to **data portability**
  8. Right to **object**

The EU Approach

The General Data Protection Regulation (GDPR)

- **Rights of data subjects:**
  1. **Transparent info** & comms to exercise data rights
  2. Right of **access**
  3. Right to **rectification**
  4. Right to **erasure**
  5. Right to **restriction of processing**
  6. Right to **notification**
  7. Right to **data portability**
  8. Right to **object**
  9. Right not to be subject to a decision based solely on **automated processing/profiling** which produces legal effects on or significantly affects the data subject…

Now back to the US…



State data protection laws

California Consumer Privacy Act

- **<u>Five key rights of CA consumers:</u>**

  1. To know what consumer personal information is collected by businesses.

  2. To know whether the personal information is sold or disclosed, and to whom.

  3. To prohibit the sale of their personal information.

  4. To access their personal information.

  5. To equal service and price, even if they exercise privacy rights under the CCPA.

State data protection laws

California Consumer Privacy Act

- **Entities:** Applies to entities that:
  - Have at least $25M in annual revenue; or
  - Receive/buy/sell/share, for commercial purposes, personal information of ≥50K CA consumers, households, or devices; or
  - Derives >1/2 of their annual revenue from the sale of personal information.
- **Personal information**: "information that identifies, relates to, describes, is capable of being associated… directly or indirectly… with a a particular consumer or household.

The Federal Trade Commission

- Two primary missions:
  1. Protecting **competition**
  2. Protecting **consumers**

The Federal Trade Commission

- The FTC Act empowers the FTC to **investigate** and **prevent** "**unfair or deceptive** acts or practices affecting commerce."
  - Via **enforcement actions** that can require companies to take specific steps, like:
    - implementation of comprehensive privacy and security programs,
    - regular audits by independent experts,
    - monetary redress to consumers,
    - disgorgement of ill-gotten gains,
    - deletion of illegally obtained information,
    - providing robust transparency & choice mechanisms to consumers.
- The FTC also has authority to obtain specific monetary penalties for violations of certain privacy statutes (e.g., COPPA).

The Federal Trade Commission

When are security/privacy practices **unfair** or **deceptive**?

Wyndham Hotels
(2015)

Equifax Breach
(2019)

Cambridge Analytica
(2019)

Zoom
(2021)

<u>In groups, consider for your case:</u>

1. What was the security/privacy practice that the FTC challenged?
2. Was it **unfair**, **deceptive**, or **both**?
   - How did the FTC argue that it was unfair/deceptive? *(Summarize in a sentence or two.)*
3. What were the **requirements** and **penalties** enforced?

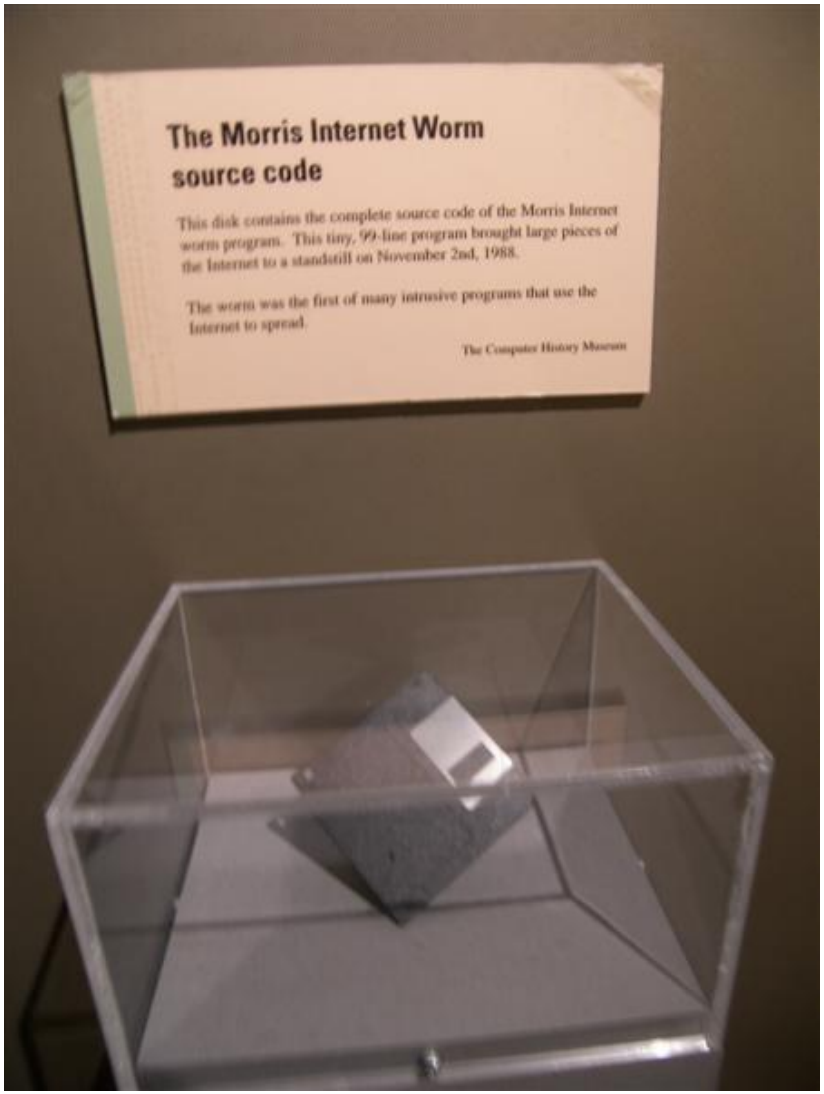
2. Computer crime law

The Computer Fraud & Abuse Act

The federal anti-hacking statute

- Prohibits “intentionally **access[ing]** a computer **without authorization** or **exceed[ing] authorized access**.”
- Also prohibits DDoS attacks, transmitting malware, etc.
- A CFAA violation can result in both civil and criminal liability.
  - Civil lawsuits can be brought by any party harmed by the access, as long as they’ve (arguably) suffered $5000 of harm.
- NB: There are state-specific anti-hacking statutes too. Many of them follow a similar high-level structure.

The Morris Worm



Critiques of the CFAA

Critiques of the CFAA

- **National Association of Criminal Defense Lawyers**: "Over the years, [the CFAA] has been amended several times… to cover a broad range of conduct far beyond its original intent. With harsh penalty schemes and malleable provisions, it has become a tool ripe for abuse and use against nearly every aspect of computer activity."

Critiques of the CFAA

- **National Association of Criminal Defense Lawyers**: "Over the years, [the CFAA] has been amended several times… to cover a broad range of conduct far beyond its original intent. With harsh penalty schemes and malleable provisions, it has become a tool ripe for abuse and use against nearly every aspect of computer activity."

- **A Supreme Court amicus brief by 18 security researchers**: "[We] are united in [our] concern that the government's broad interpretation of the [CFAA] chills essential computer security research by exposing computer security researchers to criminal and civil liability."

Critiques of the CFAA

- **National Association of Criminal Defense Lawyers**:
  "Over the years, [the CFAA] has been amended several times… to cover a broad range of conduct far beyond its original intent. With harsh penalty schemes and malleable provisions, it has become a tool ripe for abuse and use against nearly every aspect of computer activity."

- **A Supreme Court amicus brief by 18 security researchers**:
  "[We] are united in [our] concern that the government's broad interpretation of the [CFAA] chills essential computer security research by exposing computer security researchers to criminal and civil liability."

- **Electronic Frontier Foundation**:
  "After the tragic death of programmer and Internet activist Aaron Swartz, EFF calls to reform the infamously problematic [CFAA]. Creative prosecutors have taken advantage of this confusion to bring criminal charges that aren't really about hacking a computer, but instead target other behavior prosecutors dislike."

Of course,
none of this is
“legal advice.”

Of course,
none of this is
“legal advice.”

The end.