

The Right to Data Privacy

Anthony Volini

Professor of Legal Practice

Reg. Patent Attorney, CIPP/US, CIPP/E, MS Cybersecurity

The Right to Data Privacy

- ***The Right to Data Privacy: Revisiting Warren & Brandeis*, VOLUME 21 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY (2023)**
- In this PPT, I will limit citations. See my article for more details.

This talk:

- 1. Ideas from my article (mostly)
- 2. What's next? (your ideas?)

- From Disney's Frozen II, Olaf: advancing technology is both our savior and our doom!



- We're all currently asking what benefits and privacy harms or other harms AI might bring us!

The problem:

- The law struggles adapting to new technology advances (including information privacy in particular)
- **1890 problem**: the birth of mass media (faster photography and newspaper printing). Copyright, defamation concerns, biased media.
- **Today's problems**: e.g., similar but add *data collection*, AI bias, etc.
 - Too much personal data held by one party?
 - Too much personal data pumped into ecosystem of private + national security/domestic law enforcement databases?

The Solution?

- Create a suitably broad/flexible law to adapt to technology changes.
- A failing endeavor? (e.g., American Privacy Rights Act)
- Limited scope of new bills/laws (address consumer privacy but not criminal context).
 - E.g.,. Law enforcement purchasing location information bypassing warrant requirement of Carpenter.

My overly ambitious solution

- Enact a constitutional information privacy amendment, guaranteeing protection from information privacy abuse committed by government, private actors, or the two working together.
- Limit the scope to *information* privacy
- Extremely difficult to enact, but various *benefits*
- Allow states to determine private right of action (less preemptive effect if limited to *information* privacy)?

Limit scope to information privacy

- **Decisional privacy** is distinct from **information privacy**
 - **Decisional privacy**: deciding whether to have an abortion
 - **Information privacy**: Government investigating whether a person had an abortion
 - **Decisional privacy**: arguably not a privacy right at all. Arguably an individual liberty (like right to travel, free speech, assembly, reproduction, etc.).

Why is information privacy an important liberty?

Individual Liberties	
Decisional: Right to free speech Travel Assembly Reproductive rights	Information privacy: Freedom from oppressive surveillance (information about us: identity, location, religious/philosophical beliefs, finances/campaign contributions, sexual orientation/preferences, health)

- Fourth Amendment is essentially a privacy law. Consider an inmate's cell routinely searched (absence of freedom).
- Authoritarian regime tends to have mass surveillance.

Benefits of a broad/flexible information privacy amendment

- Harmonize with EU Charter of Fundamental Rights & GDPR (broad right both civil and criminal context)
- **Fill gaps** in the law rather than waiting for state/federal legislatures to act (empower courts)
- **Override other laws**: privacy abuses ostensibly protected by other laws
- Avoid **statutory interpretation conflicts**
- Avoid courts needing to **imply** an information privacy right
- Establish a baseline for any further legislation (and a baseline for courts to develop precedent). Slow down the patchwork of statutes?
- **Strong/broad/flexible legal protection** needed to address advances in technology

Strong legal protection needed

- Neither governments nor private actors can be trusted with personal data.
- Natural tendency to focus on crime detection and profits, respectively.

Flexible protection

- Why a broad and flexible law/right of protection?
- Answer: Difficult or impossible to craft detailed legislation for unknown future privacy harms.
- With the explosion of AI, broad flexible protection against information privacy abuse preferable to detailed regulations on unknown future uses of AI?
 - We're struggling to understand AI and its current/future implications
 - AI could potentially reidentify individuals using anonymized or pseudonymized data
 - AI could use public data available for one purpose that is then repurposed for some other purpose. (Contextual Integrity problem.)
 - A predictive policing practice was found unconstitutional by the German Constitutional Court, finding it violated a broad right to informational self-determination. (Could US benefit from a similar broad right?)
 - 2002 film Minority Report: specialized "precrime" police force arrested criminals before commission of a crime. Seems far-fetched, but police departments around the country use surveillance and predictive policing tools every day.

Gap filling

- *See In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125 (3d Cir. 2015) (ruling that dismissal of a variety of federal and state claims was appropriate but that plaintiffs' **California Constitutional privacy claim should survive dismissal**); *see also In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020) (affirming the district court's dismissal of the SCA, breach of contract, and breach of implied covenant claims, but ruling that Plaintiffs adequately pleaded their remaining claims (e.g., California Constitutional invasion of privacy claim and common law intrusion upon seclusion)).

Override other laws with constitutional protection

- **Mug shots.** Illinois & other states passed legislation to stop websites from charging fees for removing a person's published mugshots. Websites had asserted newsworthiness in defense of this practice.
- A court could have viewed this as an information privacy abuse **without the need for legislation**, especially with strong constitutional protection.
- **Communications Decency Act.** Websites allowing anonymous defamatory posts about individuals alleging that they are cheaters, drug users, etc. and charging a fee to remove the content. Website asserts no liability as a protected platform under CDA. A constitutional amendment could override such asserted protection as unconstitutional.
- **Another example:** California Supreme Court found a California parental consent statute in the abortion context violated the California Constitutional right to privacy. *Am. Acad. of Pediatrics v. Lungren*, 940 P.2d 797, 831 (Cal. 1997).

Avoid statutory interpretation conflicts

- A later enacted statute might not override a prior statute in some situations?
- A broad statutory right might create potential conflicts with other statutes and thus interpretation challenges. See Steve R. Johnson, *When General Statutes and Specific Statutes Conflict*, 57 ST. TAX NOTES 599 (2010), Available at: <https://ir.law.fsu.edu/articles/304> (discussing interpretation of conflicting statutes, such as more recent statutes overriding prior statutes, but more specific statutes outweighing general statutes).
- (I have not explored this concept much regarding existing privacy laws.)

Judicial reluctance to imply an information privacy right?

- Post Dobbs. A concern?
- Dobbs (dissent) mentioned a contraction of one right may lead to a contraction of other rights. Hence, a broad powerful information privacy right would be helpful?
- The federal government post Patriot Act greatly reduced financial privacy. Post-Dobbs, possibility of states attempting long arm jurisdiction to prosecute out of state abortions (discovery of financial transactions and other data)

What's next?

- Assess state constitutions with a privacy right?
- Are they focused on information privacy?
- How effective are they at filling gaps, overriding other laws, etc.?
- Assess prior tech laws becoming obsolete with changes in technology?
- Explore effectiveness of a statute as an alternative?
- What else?????????

Thank you!

- Questions? Comments?
- Feel free to reach out avolini@depaul.edu