Sebastian Zimmeck
Wesleyan University

Structural Compliance: Making Software Systems Inherently Lawful

4th Anonymity Day
Joyce Cummings Center, Tufts University

June 3, 2026

Three Research Projects

1) Apps: Mobile App Privacy Compliance
2) Web: Global Privacy Control
3) AI Models: XAI Privacy

=> Structural Compliance

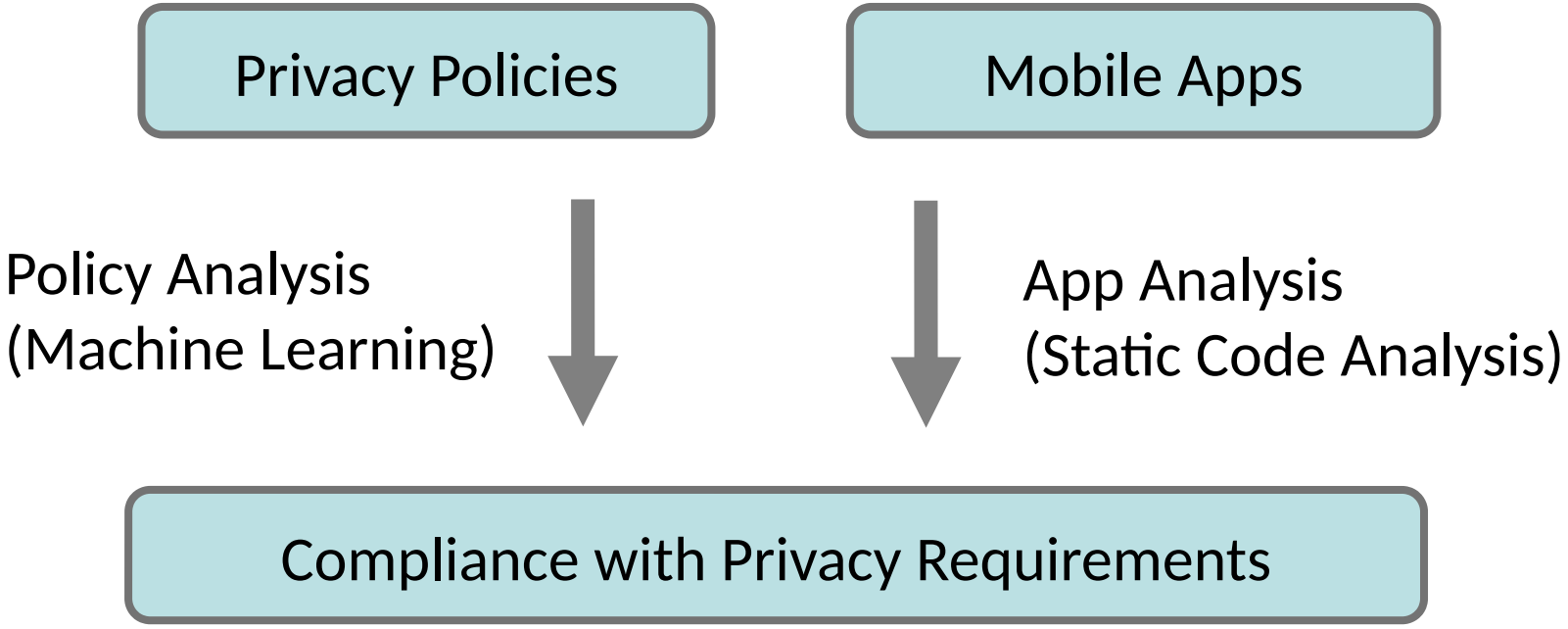
Project 1: Apps
Mobile App Privacy Compliance

Motivation

The California Online Privacy Protection Act requires app publishers to have a privacy policy and transparently disclose data practices (California Business and Professions Code Sections 22575-22579)

→ System to evaluate how many apps have a privacy policy, whether the policies follow legal requirements, and analyze discrepancies between apps and policies

Compare App Behavior to Privacy Policies



Project 2: Web
Global Privacy Control

GPC signal detected. Test against the **reference server** .

GLOBAL PRIVACY CONTROL

ABOUT SPEC FOR USERS FOR IMPLEMENTERS DOWNLOAD ORGANIZATIONS PRESS FAQ

Take control of your privacy.

Online privacy should be accessible to everyone. It starts with a simpler way to exercise your rights.

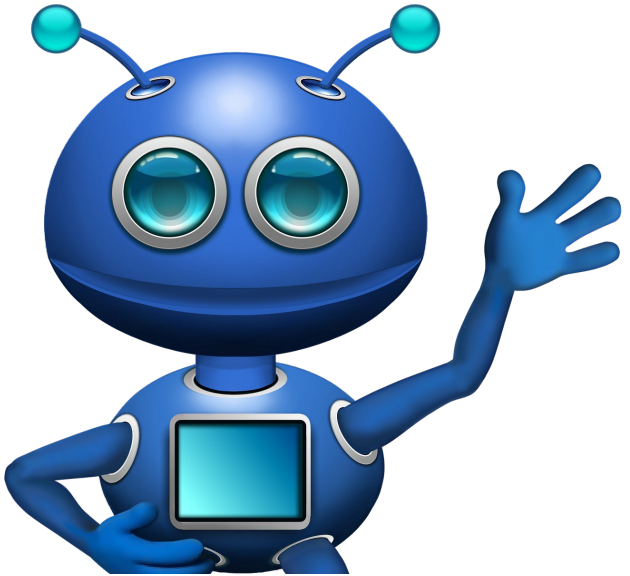
GET STARTED

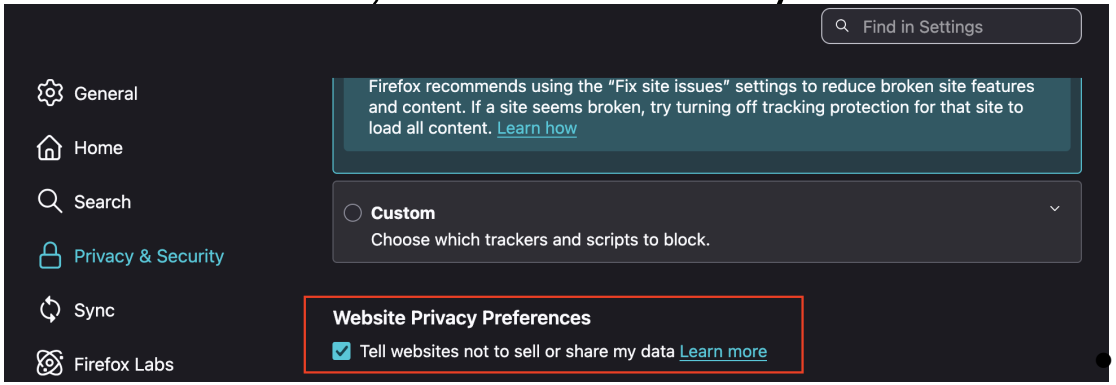
GET INVOLVED

https://globalprivacycontrol.org/

What is GPC?

- Global Privacy Control (GPC) is like a little robot sending a do-not track signal
- For all sites you visit or just some
- For web, mobile apps, …
- Wait a minute, don't we already have DNT?





- Firefox 147.0.1 GPC setting

GPC project site: https://globalprivacycontrol.org/

Archive - Attorney General Becerra
@AGBecerra

#CCPA requires businesses to treat a user-enabled global privacy control as a legally valid consumer request to opt out of the sale of their data.

CCPA opened the door to developing a technical standard, like the GPC, which satisfies this legal requirement & protects privacy.

6:56 PM · Jan 28, 2021

2026 Press Releases
2025 Press Releases
Attorney General Tong Announces Coalition of State Attorneys General
2024 Press Releases
2023 Press Releases
2022 Press Releases
2021 Press Releases
2020 Press Releases
2019 Press Releases

Search Office of the Attorney General
by Keyword

Press Releases

OFFICE OF THE ATTORNEY GENERAL
CONNECTICUT

09/09/2025

Connecticut, California and Colorado Announce Joint Investigative Privacy Sweep

States Investigating Businesses Refusing to Honor Consumers' Right to Opt-Out of the Sale of Their Personal Information

(Hartford, CT) — Connecticut Attorney General William Tong and the attorneys general of California and Colorado and the California Privacy Protection Agency today announced an investigative sweep involving potential noncompliance with Global Privacy Control, or GPC, an easy-to-use browser setting or extension that automatically signals to businesses a consumer's request to stop selling or sharing their personal information to third parties. As part of the sweep announced today, the coalition sent letters to businesses that do not appear to be processing consumer requests to opt out of the sale of their personal information submitted via the GPC as required by law and requested that those businesses come into immediate compliance. This sweep reinforces the three states' 2025 Data Privacy Day **educational efforts** on the

Integrating GPC into the Structure of the Web

TABLE OF CONTENTS

Global Privacy Control (GPC)

ReSpec

Proposal 22 March 2024

▾ **More details about this document**

Latest editor's draft:
https://privacycg.github.io/gpc-spec/

History:
Commit history

Editors:
Sebastian Zimmeck (Wesleyan University)
Peter Snyder (Brave Software)
Justin Brookman (Consumer Reports)
Aram Zucker-Scharff (The Washington Post)

Former editors:
Robin Berjon (Protocol Labs) (The New York Times until Sep 2022)
Ashkan Soltani (Independent)
David Harbage (DuckDuckGo)

Feedback:
GitHub privacycg/gpc-spec (pull requests, new issue, open issues)

Copyright © 2024 the document editors/authors. Text is available under the Creative Commons Attribution 4.0 International Public License; additional terms may apply.

Abstract

This document defines a signal, transmitted over HTTP and through the DOM, that conveys a person's request

GPC specification: https://w3c.github.io/gpc/

Project 3: AI Models
XAI Privacy

Motivation

Make
AI Models Compliant
with the Law

Case Study: Disaster Relief

Scenario

The Texas Division of Emergency Management (TDEM) intends to create a grant system for homeowners to hurricane-proof their properties.

TDEM creates an environmental risk score applied by an AI system to pre-screen each grant application.

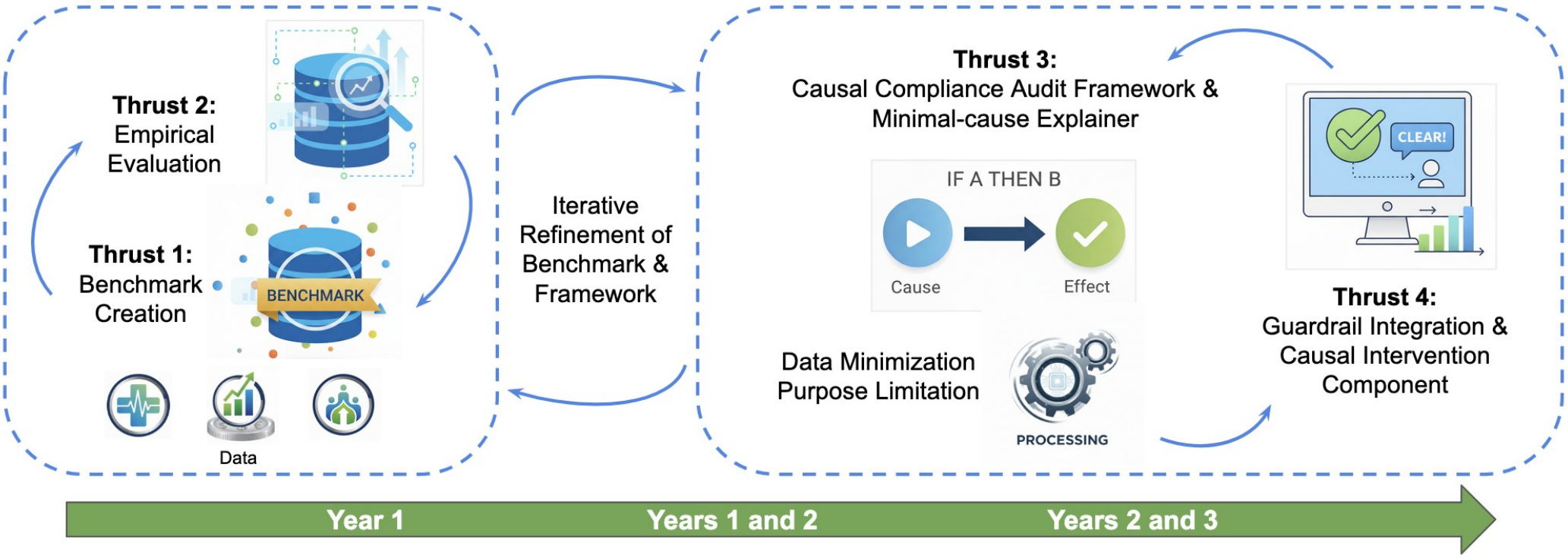
Causality

Law

Section 552.053, Texas Responsible AI Governance Act

"A governmental entity may not use ... an artificial intelligence system that evaluates ... a natural person ... based on social behavior or personal characteristics ... with the intent to calculate ... a social score ... that may result in: (1) detrimental ... treatment of a person ... in a social context unrelated to the context in which the behavior or characteristics were observed ..."

Research Thrusts



The Big Picture

Structural Asymmetries

- **Automation**: Data collection and use are largely automated while user protection mechanisms often require manual intervention
- **Knowledge**: Users are generally left in the dark about how their data is collected, used, and to whom it is disclosed
- **Economics**: Data often holds only minimal financial value to a single individual but aggregated at scale has substantial economic value for companies
- **Jurisdictions**: Most laws apply locally, yet the Internet and many other software systems are global
- **Enforcement**: Enforcement of laws is reactive and happens on an individual basis while non-compliance happens as a system emerges on a broad scale

Upholding the Rule of Law Online

- **The Legal Deficit**: If software systems do not behave according to the law, we can not fully realize their full potential, especially, for sensitive tasks (e.g., healthcare, employment)
- **Why build law into systems?** To ensure that the rule of law is effective and efficient online instead of dealing with two separate worlds
- **“Code is (Mostly Not) Law”**: Left to itself, software architecture prioritizes optimization and engagement, not democratic legal norms
- **The Objective**: Evolve systems so that they inherently adheres to the law through their very design

Defining Structural Compliance

- **What is Structural Compliance?** A system design concept that ensures a system's technological structure inherently guarantees behavior that aligns with legal norms

- **Related concepts**:

1) **Privacy by Design**: Structural compliance extends beyond privacy and does not require that a system's initial design is compliant but that it can be retrofitted

2) **Code is Law**: Code does not displace legal systems but structural compliance uses code as an execution and enforcement mechanism to satisfy applicable laws

3) **Contextual Integrity (CI)**: Structural compliance can leverage CI to determine the context boundaries where a law should be applied

- **System Properties vs. System Behaviors**: Structural compliance relies on technical system properties (e.g., differential privacy) to guarantee specific behavior compliant with the law (e.g., anonymity, transparency, or data minimization)

What Systems Are We Talking About?

- **The Web and Internet**: E.g., exercising opt-out rights via built-in opt-out mechanisms like GPC
- **AI Models**: E.g., guardrails for not disclosing personal data used for training
- **Hardware and physical infrastructure?**

The “Translation” Task: Law as a Software Development Artifact

- A major challenge lies in the “**translation**” of legal prose into quantitative criteria and executable code (“Where is the science?”)
- **Traceability**: Establishing a verifiable pipeline from a high-level legal statute down to system specifications and implementations
- **Privacy Policies as Software Development Artifacts**: E.g., generating privacy policies from mobile app code (“Who is responsible?”)
- **Different Mappings:** A single technical mechanism may require entirely different legal mappings depending on the jurisdiction in which it is applied

Structural Compliance vs. Innovation

- **The Risk of Stifling Innovation:** If a system is unyielding, it loses the flexibility necessary for updates, evolution, and innovation
- Simply “**hardcoding**” laws is also disadvantageous as it risks freezing systems in time
- **The Challenge**: How do we build systems that are structurally lawful yet dynamically flexible?

Bridging Law and Code

- **Decoupling Law and Code**: Laws change slowly through legislative processes; systems are developed and evolved much faster. They cannot be directly coupled
- **Mediators (Steps for the Bridge)**: Technical standards (e.g., at the W3C), regulations, or even just FAQs on a state attorney general website act as flexible abstraction layer(s) between statutory requirements and code implementation
- **Living Standards, Regulations, etc.**: They can be dynamically evolved to adapt to new system capabilities, threats, and user needs

Co-Designing Law and Technology

- **Lawmaking**: While natural language is inherently vague and ambiguous, legislate with an eye towards technological feasibility
- **Enforceability**: Future laws should be written with automated enforcement in mind, supporting the creation of technical standards
- **Agency Regulation**: Regulatory agencies can use administrative rulemaking to provide necessary elasticity from the legal end to match standards
- **Structural Compliance Requirement**: Law can require structural compliance

Why Implement Law into Systems?

- **Laws Give People Rights**: Privacy, Anonymity, ...
- **Values Behind Rights**: Personal Autonomy, …
- Computer Science moves to **higher level of abstraction**

Thank You!

Questions and Discussion

Sebastian Zimmeck, szimmeck@wesleyan.edu