**Call for Presentations:** PrivacyCon 2021

**first and last name:** Craig Erickson

**email address:** craig-erickson@privacyportfolio.com

**phone number:** (510) 330-8638

**job title:** Data Protection Officer

**affiliation of researcher(s) making the request:** PrivacyPortfolio

**single point of contact for communications with FTC staff**: Craig Erickson

**title of the research:** "Crowdsourced Compliance Platforms Keep Enforcement Authorities Honest"

**covered areas of interest:**

* Consumer Demand for Privacy and Security
* Consumer Behavior Related to Privacy and Security Risks
* Consumer Beliefs and Attitudes Related to Privacy and Security
* Effectiveness of Consumer Privacy and Security Disclosures
* Privacy-Enhancing Technologies for Consumers
* Company Incentives and Behavior Regarding Privacy and Security Practices
* Privacy and Security of Health Data

**how your research differs from prior research in this area:** To the best of my knowledge, there is no research regarding how effectively enforcement authorities investigate consumer complaints about denial and obstruction of consumers’ privacy rights.

**publication details for any research that has been previously published or accepted for publication:** *Crowdsourced Compliance: Managing customer audits at scale*

2019 presentation at ISACA-Silicon Valley Spring Conference <https://privacyportfolio.com/slides/CrowdsourcingCompliance.pdf>

**additional information you would like to share**:

Most of my research is published in my open data catalogs as a series of privacy experiments, in which published tests are conducted and test results are published as evidence within the context of an individual California consumer's use of a Vendor Risk Platform to evaluate the practices of organizations possessing the consumer's personal information.

**Any sources of funding for your research:** Self-funded by PrivacyPortfolio

**request for confidential treatment:** No request submitted

**completed or draft research paper or extended abstract:**

PrivacyPortfolio represents consumers as their authorized privacy agent, providing consumers with standardized tests and collection of evidence supporting the denial or obstruction of their privacy rights. This service goes beyond submitting privacy requests on behalf of the consumer by submitting consumer complaints to states attorney generals, evaluating the AG's performance investigating these complaints. The complaints and any responses are published in a public "evidence" dataset for transparency.

**Methodology used** is typical of vendor risk assessments commonly used by businesses to vet their third-party providers, but in lieu of reviewing SOC2 reports, Data Privacy Impact Assessments and issuing self-assessment questionnaires, the vendors' privacy practices and controls are tested directly by consumers, using techniques similar to those utilized by ethical hackers conducting penetration tests.

**Findings include:**

1. Only 1 out of 68 consumer complaints was investigated by the CA OAG.
2. Regarding the one case investigated, the CA OAG did not review the published evidence, but instead accepted the vendor's word that their internal team discovered no regulatory issues.
3. One case study involving Alphabet's Verily Life Sciences, Google, Chronicle, and Project Baseline, illustrates how businesses position themselves as being exempt from HIPAA and exempt from the CCPA as service providers, while collecting extremely invasive mental health information, which is permitted when "finding and recruiting qualified participants for medical studies". Craig Erickson, a California consumer joined Project Baseline when the pandemic hit the US in March 2020, in pursuit of a COVID-19 test when opportunities were extremely limited. Third-parties used by Project Baseline included the California Department of Public Health (CDPH), IDology, Quest Diagnostics, Optum360, PWNHealth, WCGClinical (WIRB), and RiteAid. Craig Erickson made every attempt to follow the flow of this sensitive personal data using privacy requests to all entities and captured screenshots, cookies, and other documents in the course of applying for clinical studies on Project Baseline’s platform. Project Baseline and all of Project Baseline’s "partners" with the exception of WCGClinical, were completely opaque about their relationship with Project Baseline, and would not comment on Project Baseline's assertions made on behalf of these partners, as to whether their products and services were used for the stated purposes.

**Summary**:

* Law enforcement relies heavily on tips from the public regarding criminal and fraudulent activities.
* Greater public participation in reporting privacy violations could increase overall compliance with privacy law.
* Consumers can use simple methods to gather objective, reproducible, and non-anecdotal evidence.
* Unlike the FTC, consumers cannot follow complex the flow of data between diverse entities to determine fraud.
* Leveraging open datasets provided by citizens as input to FTC investigations, could further incentivize the public’s participation in reporting violations of privacy law.

The combination of better public reporting methods, along with greater transparency about the effectiveness of enforcement authorities, could substantially improve the cost-effectiveness of enforcing overall compliance with existing privacy regulations.