Compliance Crowdsourcing: Managing customer audits at scale

Craig Erickson, CISSP, CISA
Data Protection Officer, PrivacyPortfolio
Crowdsourcing
Crowdsourcing is a sourcing model in which individuals or organizations obtain goods and services, including ideas and finances, from a large, relatively open and often rapidly-evolving group of internet users; it divides work between participants to achieve a cumulative result.
HOW ENTERPRISES CAN BENEFIT FROM CROWD ENGAGEMENT

SYSTEMS
IT + Communications + Security
NEED: Assurance
BENEFITS: Identify and Mitigate Cyber-Threats, Outsourcing Opportunities, Improve ICT Use

OPERATIONS
Production + Delivery + Service
NEED: Improvement
BENEFITS: Supply Chain Efficiencies, Quality, Competitive Advantage

INNOVATION
Product Management + R&D
NEED: Progress
BENEFITS: Creativity / Ideas, User-Driven Design, Collaborative Partnering

FINANCE
Accounting + Procurement + Payroll
NEED: Optimization
BENEFITS: Capital, Cost Reduction, Risk Mitigation, Outsourcing Opportunities

GOVERNANCE
Owners/Investors + Executives
NEED: Value
BENEFITS: Equity-effective Funding, Improved ROI, Enhanced Cx & Valuations

CULTURE
Human Resources Management
NEED: Effectiveness
BENEFITS: Improved Learning & Transformation, Recruiting Opportunities, Employer of Choice

COMMERCIAL
Marketing + Sales + CRM
NEED: Growth
BENEFITS: New Leads, Marketplace Engagement & Customer Experience

2019 ISACA-SV Spring Conference
Where Can Crowdsourcing Be Applied?

Governments are applying crowdsourcing to empower citizens and give a greater voice to the people.

In science and health care, crowdsourcing can democratize problem solving and accelerate innovation.

With education, it has the potential to revolutionize the system, just as crowdfunding is currently challenging traditional banking and investing processes.

It’s a 21st-century mindset and approach that can be applied in many areas and many ways...
Shift toward “customer-centric” models... 
... and away from enterprise “top-down” models

• Customers trust other customers’ opinions more than they trust experts;
• The standards and practices we’ve established in our profession aren’t shared by consumers;
• Changing norms threaten existing shared values;
• Consumers increasingly feel *dictated to* and *manipulated* and market trends are trying to exploit this sentiment.
Now, Consumers Set the Standards
Consumer Reports Launches Digital Standard to Safeguard Consumers' Security and Privacy in Complex Marketplace

New initiative to measure the privacy and security of products, apps, and services will put consumers in the driver's seat as the digital marketplace evolves

Filed under: Policy & Mobilization, Electronics, Organizational News
Release date 03/06/2017
The Digital Standard

https://www.thedigitalstandard.org/

About the Standard

[The Digital Standard](https://www.thedigitalstandard.org/) is an ambitious, community-led effort to build a framework to test and rate products and services on the basis of privacy, security, and data practices.

Consumers care about digital privacy and security but often have no way to understand how a product or service treats and protects their data. While there are established criteria and tests to measure fuel efficiency in cars, the crash performance of car seats, and the energy efficiency of home appliances, consumer organizations currently lack standards for testing and rating how well products and services manage consumers’ privacy, security, and data. These issues are big, pressing, and not fully understood, but will define product and service quality and accountability in the 21st century and standard tests and ratings must now be developed.
2019 ISACA-SV Spring Conference
Advertisers get ads. Period.

There's no amount of money a business can pay to manipulate their reviews or rating and Yelp doesn't skew things in favor of advertisers or against businesses that don't.

But you don't have to take our word for it.

An independent academic study (not commissioned or paid for by Yelp) found that **advertising plays no role in how reviews are recommended** on Yelp. Or as this *in-depth profile of Yelp in BuzzFeed* puts it: "Harvard Business School professor Michael Luca has co-authored a new study that effectively **debunks the extortion theory**."

Conspiracy theorists have had their day in court on more than one occasion, but courts have repeatedly dismissed their lawsuits claiming that ratings and reviews on Yelp are somehow tied to advertising. The FTC also concluded a year-long investigation of similar claims without taking any action. You can find the media reports here: PC World, WSJ, HuffPost, CNET, LA Times, CNN Money.

* If we included “Data Quality” as one metric, we’d find the ‘new study’ is 8 or 9 yrs old...
RDR Corporate Accountability Index

The RDR Corporate Accountability Index evaluates the world’s most powerful internet, mobile, and telecommunications companies’ disclosed policies and practices affecting users’ freedom of expression and privacy. The 2019 Index will be released in May 2019.

May 16: Global Launch of the 2019 Ranking Digital Rights Corporate Accountability Index!
Key findings

17 of the 22 companies evaluated for the 2018 Index improved scores in at least one area, and many made multiple improvements in the past year. Yet companies still fall short:

- Privacy: Companies fail to disclose enough about what user information is collected and shared, with whom, and under what circumstances.

- Security: Companies provide insufficient evidence of measures to protect users’ information.

- Expression: Companies keep the public in the dark about how content and information flows are policed and shaped through their platforms and services.

- Governance: Too few companies make users’ expression and privacy rights a central priority for corporate oversight, governance, and risk assessment.

The 2018 Index ranks 22 companies on 35 indicators across three categories evaluating how transparent companies are about commitments and policies affecting freedom of expression and privacy. The Index evaluates policies of the parent company, operating company and those of selected services (depending on company structure).

Read more about the methodology, research process and how we score each company.

READ THE EXECUTIVE SUMMARY
READ OUR RECOMMENDATIONS
DOWNLOAD THE FULL REPORT
1. 2018 Index Methodology

The 2018 Index measures company disclosure of policies and practices affecting users’ freedom of expression and privacy. The Index methodology applies 35 indicators in three main categories: Governance, Freedom of Expression, and Privacy. Each category contains indicators measuring company disclosure for that category; each indicator is comprised of a series of elements that measure company disclosure for that indicator.[9]

1.1. Index categories

- **Governance [G]**: This category contains six indicators measuring company disclosure of commitments to freedom of expression and privacy principles along with measures taken to implement those commitments across the company’s global operations.[10]

- **Freedom of Expression [F]**: This category contains 11 indicators measuring company disclosure of policies that affect users’ freedom of expression.[11]

- **Privacy [P]**: This category contains 18 indicators measuring company disclosure of policies and practices that affect users’ privacy rights.[12]

1.2. Company types

While every company we examined has attributes that make it unique, for the purpose of research and scoring, we divided the 22 companies into two groups.

**Internet and mobile ecosystems**: This category includes both internet companies and companies that produce software and devices that we call “mobile ecosystems.” These company types are evaluated together because Google is both an internet company and a mobile ecosystem company, and along with its iOS mobile ecosystem, Apple also offers services like iMessage and iCloud. In addition, the freedom of expression and privacy issues faced by mobile cloud data and operating systems overlap with the issues faced by traditional internet services. We do not evaluate hardware attributes of devices, focusing our assessment instead on their operating systems. Additional elements relevant only to mobile ecosystems were added to some indicators.
Now, Consumers Test the Controls
Here’s an idyllic vision...

We work for a fair, just, and safe software marketplace for all consumers, empowering consumers to protect themselves.

When do we get our pitchforks?
A Self-Managed HackerOne Bug Bounty Program

Use your abundant resources and past experience to run your own bug bounty program.

1. Hacker searches for vulnerabilities
2. Hacker submits it to your organization
3. Your team works closely with hackers to receive all relevant data
4. Your security staff validates all vulnerability reports
5. Your security team triages all submissions and fixes all valid submissions

Managed by HackerOne • Managed by You

2019 ISACA-SV Spring Conference
Tweets by @darkpatterns

Alex Tokmakchiev @atomakchiev
@darkingpatterns Try and figure out how to cancel your subscription for @GanttPROcom. Yep it's the little "link" word that has a font-size of 11px and in no way looks like a link.

Also, it's mentioned nowhere in their Help Center (which conveniently has no search).

2019 ISACA-SV Spring Conference
P: Privacy

Indicators in this category seek evidence that in its disclosed policies and practices, the company demonstrates concrete ways in which it respects the right to privacy of users, as articulated in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and other international human rights instruments. The company’s disclosed policies and practices demonstrate how it works to avoid contributing to actions that may interfere with users’ privacy, except where such actions are lawful, proportionate and for a justifiable purpose. They will also demonstrate a strong commitment to protect and defend users’ digital security. Companies that perform well on these indicators demonstrate a strong public commitment to transparency not only in terms of how they respond to government and others’ demands, but also how they determine, communicate, and enforce private rules and commercial practices that affect users’ privacy.

P1. Access to privacy policies

The company should offer privacy policies that are easy to find and easy to understand.

Elements:

1. Are the company’s privacy policies easy to find?
2. Are the privacy policies available in the language(s) most commonly spoken by the company’s users?
3. Are the policies presented in an understandable manner?
4. (For mobile ecosystems): Does the company disclose that it requires apps made available through its app store to provide users with a privacy policy?

P2. Changes to privacy policies

The company should clearly disclose that it provides notice and documentation to users when it changes its privacy policies.

Elements:

1. Does the company clearly disclose that it notifies users about changes to its privacy policies?
2. Does the company clearly disclose how it will directly notify users of changes?
3. Does the company clearly disclose the time frame within which it provides notification prior to changes coming into effect?
Privacy Portfolio

About Us | Our Policy | Your Choices

description: Statements | Claims | Rules

This privacy policy represents claims and rules pertaining to PrivacyPortfolio's privacy practices.

XSLT

2019 ISACA-SV Spring Conference
Rule provisions access to API tests

Policy Changes

PrivacyPortfolio will change this Policy periodically based on changes to applicable laws and regulations or changes in technology or our business operations.

Changes we make to the Policy in the future will:
1) change the policy version and effective date;
2) be posted as an update on our web page at privacyportfolio.com;
3) and if you have subscribed to changes in our policies or terms of service, we will notify you directly according to your communication preferences.

Rule: policyChanges
Value: [not set]
Objective: list differences between two policy instances
Context: Subscriber
Standard: policy format must be the same for both policy instances to compare
Test: list = policyChanges(policy p1, policy p2)
Evidence: online test results

2019 ISACA-SV Spring Conference
Privacy Process Flow

1. Capture Policy
2. Compare Policy
3. Create Agreement
4. Provision Access
5. Audit Access
6. Test Policy
7. Monitor Publisher
8. Publish Results

Consumer As Subscriber

1. Publish Policy
2. Negotiate Policy
3. Sign Agreement
4. Provision Access
5. Audit Access
6. Test Policy
7. Monitor Subscriber
8. Publish Results

Organization As Publisher

2019 ISACA-SV Spring Conference
Consent Receipt Specification

Version: 1.1.0
Document Date: 2018-02-20

Editors: Mark Lizar, David Turner
Contributors: Richard Beaumont, Chris Cooper, Sal D’Agostino,
Rupert Graves, Iain Henderson, Mary Hodder,
Harri Honko, Andrew Hughes, Tom Jones,
Robert Lapes, Oliver Maerz, Eve Maler, Jim Pasquale,
Samuli Tuoriniemi, John Wunderlich

Produced by: Consent & Information Sharing Work Group

Status:
This document is a Kantara Initiative Technical Specification Recommendation produced by the Consent & Information Sharing Work Group, and has been approved by the Group. The Public Comment and Intellectual Property Rights Review has been completed. It has been approved by the Membership of the Kantara Initiative. See the Kantara Initiative Operating Procedures for more information.

Abstract:
A Consent Receipt is record of authority granted by a Personally Identifiable Information (PII) Principal to a PII Controller for processing of the Principal’s PII. The record of consent
Now, Consumers Have the Evidence
“(12) STATISTICAL PURPOSE.—The term ‘statistical purpose’— means the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups.

(1) ACCURATE.—The term ‘accurate’, when used with respect to statistical activities, means statistics that consistently match the events and trends being measured.

(2) CONFIDENTIALITY.—The term ‘confidentiality’ means a quality or condition accorded to information as an obligation not to disclose that information to an unauthorized party.

(3) OBJECTIVE.—The term ‘objective’, when used with respect to statistical activities, means accurate, clear, complete, and unbiased.

(4) RELEVANT.—The term ‘relevant’, when used with respect to statistical information, means processes, activities, and other such matters likely to be useful to policymakers and public and private sector data users.

“(19) the term ‘metadata’ means structural or descriptive information about data such as content, format, source, rights, accuracy, provenance, frequency, periodicity, granularity, publisher or responsible party, contact information, method of collection, and other descriptions;
On January 14, 2019, the Foundations for Evidence-Based Policymaking Act ("Evidence Act"), which includes the OPEN Government Data Act, was signed into law. The Evidence Act requires the Office of Management and Budget, the Office of Government Information Services, and the General Services Administration to develop and maintain an online repository of tools, best practices, and schema standards to facilitate the adoption of open data practices across the Federal Government. When the new repository is launched, it will replace and retire Project Open Data. Check back here for updates.

Slash Data Catalog Requirements

This section provides further guidance and explanation for implementing the agency data catalog.

/Data Requirements

The Open Data Policy requires agencies to list and describe all agency data that can be made publicly available (i.e. there are no valid restrictions to release) in a publicly available open data catalog using the Project Open Data metadata schema. It further requires the catalog to be human-readable and machine-readable. This guidance describes to agencies steps for implementing this portion of the policy.

Why this effort

The data that agencies collect and curate is a national treasure. Data from the National Weather Service and the Global Positioning System have each given rise to countless products and entire industries, yet much more government data exists, waiting to be tapped for its potential.

To this end, the Digital Strategy action item 2.2 requires agencies to catalog and tag their data to make it more easily discoverable to private-sector developers and entrepreneurs.

Through this effort, agencies will begin to tag their data, using common standards, and in the process, build a comprehensive folksonomy to make government data more easily discoverable.

Each agency will describe their existing datasets as they see fit using the below described standard, and will make this metadata available at a consistent URL across agencies. Similar to existing practices already in use on the web, such as sitemap.xml or robots.txt, this will allow developers, both within the government and the public to
Explore datasets, tools, and applications related to health and health care. These resources come from across the Federal Government with the goal of improving the health and lives of all Americans.

**HIGHLIGHTS**

**Hospital Charge Data**

Data are being released that show significant variation across the country and within communities in what providers charge for common services. These data include information comparing the charges for the 100 most common inpatient services and 30 common outpatient services. Providers determine what they will charge for items and services provided to patients and these charges are the amount the providers bills for an item or service.

**UPDATES**

**Introducing OpenFDA from the Food and Drug Administration**

March 11, 2014  By admin
3 datasets found for "organization:((osc-gov))"

Employee Information
US Office of the Special Counsel — Count of OSC employees (FTE's) on a monthly basis
Excel

Training Information
US Office of the Special Counsel — Listing of Training attended by OSC employees on a yearly basis
Excel

Printing Information for FY 2009
US Office of the Special Counsel — Listing of materials printed by OSC on an annual basis
Excel

You are searching in the list of datasets. Show results in entire Data.gov site.

You are not authorized to do this
Collaboration and Crowdsourcing

- Does the catalog support free-form tagging and commenting to allow business users to annotate data sets in a way that makes sense to them?

- Can new, better data sets be “crowdsourced,” i.e., shared, annotated, enriched, and improved—while still maintaining the integrity of the data?

Are you trying to build a more collaborative context for decision making?

Then you will want to focus your evaluation on how the data catalog can help data consumers understand the context of their data—where it has been, who owns it, who can access it, and the rules governing its use.
Crowdsourcing annotations and user perspective (multiplicity of opinion)

A key aspect of Azure Data Catalog is how it supports the crowdsourcing of metadata in the system. As opposed to a wiki approach – where there is only one opinion and the last writer wins – the Azure Data Catalog model allows multiple opinions to live side by side in the system.

This approach reflects the real world of enterprise data where different users can have different perspectives on a given asset:

- A database administrator may provide information about service level agreements, or the available processing window for bulk ETL operations
- A data steward may provide information about the business processes to which the asset applies, or the classifications that the business has applied to it
- A finance analyst may provide information about how the data is used during end-of-period reporting tasks

To support this example, each user – the DBA, the data steward, and the analyst – can add a description to a single table that has been registered in the Catalog. All descriptions are maintained in the system, and in the Azure Data Catalog portal all descriptions are displayed.
Are you trying to promote trust through better data policies and improved data quality and consistency?

Then you will want a data catalog tightly integrated with data governance capabilities which support data rules and allow you to easily configure workflows that are right for your organization.
Data Registration

- Can the catalog connect to multiple data sources and metadata repositories across your organization and access that data for immediate tasks?
- Does the catalog automatically create new metadata to make data discovery faster and easier?
- Can users be alerted when a more up-to-date version of the data set becomes available?
“Enable to Protect” – Malcolm Harkins

You’ve spent a lot of money on self-service BI, but finding the data to populate those tools is still difficult.

Your organization has numerous data sources, but data consumers have no easy way to identify those sources in one central location.

Your “let’s store everything here” data lake has turned into a murky data swamp that makes finding meaningful, trustworthy data close to impossible.

There is no process in place for data consumers to request the data they need.

Even when data consumers can access data, they don’t have information about what the data means or how it should be used.

Data consumers don’t know the source of the data they find and so cannot confirm the data’s trustworthiness.

Data consumers don’t know who ‘owns’ the data and therefore have no way to contact subject matter experts.

Data consumers don’t know what data sets already exist across the enterprise or who has used similar data to explore similar problems.
Compliance Crowdsourcing Summary

- Crowdsourcing is a growing trend, providing companies with untapped resources and more input from consumers.
- Auditors can play an important role in helping crowdsourced models be more transparent and equitable for all stakeholders, building trust.
- Consumers want to set their own standards through direct negotiations.
- Businesses want specific customer requirements they can ‘operationalize’.
- Managing data privacy rights at scale requires automated business processes for organizations and consumers, that complies with all applicable laws.
- Data Catalogs can be a valuable collaboration tool for sharing and governing data in a transparent but secure manner.
- The Open Government Data Act provides standards for evidence obtained through crowdsourcing.
BETA STARTS MAY 15