Describing and setting forth a proposal to the voters at an election to be held November 6, 2018, to amend the Charter of the City and County of San Francisco to adopt a Privacy First Policy.

Existing Law

While federal, state, and City law provide some protections for privacy in the collection, storage, sharing, and use of Personal Information, there is no overarching set of privacy-protective principles in City law.

Amendments to Current Law

The Charter amendment establishes a Privacy First Policy to provide guidance to the City when considering the adoption of privacy-protective laws, regulations, policies, and practices for the City; the City’s contractors, lessees, and grantees; third parties receiving permits, licenses, or other entitlements from the City; and persons (including businesses and other entities) within the regulatory authority of the City.

These principles constitute the Privacy First Policy:

1. Engage with and inform those likely to be impacted by the collection, storage, sharing, or use of their Personal Information prior to authorizing and prior to any change regarding the collection, storage, sharing, or use of their Personal Information.
2. Ensure that Personal Information that is collected, stored, shared, or used is done so pursuant to a lawful and authorized purpose.
3. Allow individuals to access Personal Information about themselves that has been collected, and provide access and tools to correct any inaccurate Personal Information.
4. Solicit informed consent to the collection, storage, sharing, or use of Personal Information, and provide alternative and equal access to goods and services for those who deny or revoke consent.
5. Discourage the collection, storage, sharing, or use of Personal Information, including potentially sensitive demographic information, unless necessary to accomplish a lawful, authorized purpose.
PUSH, PULL, AND SPILL: A TRANSDISCIPLINARY CASE STUDY IN MUNICIPAL OPEN GOVERNMENT
Jan Whittington, Ryan Calo, Mike Simon, Jesse Woo, Meg Young & Peter Schmiedeskamp

ABSTRACT

Municipal open data raises hopes and concerns. The activities of cities produce a wide array of data, data that is vastly enriched by ubiquitous computing. Municipal data is opened as it is pushed to, pulled by, and spilled to the public through online portals, requests for public records, and releases by cities and their vendors, contractors, and partners. By opening data, cities hope to raise public trust and prompt innovation. Municipal data, however, is often about the people who live, work, and travel in the city. By opening data, cities raise concern for privacy and social justice.

This article presents the results of a broad empirical exploration of municipal data release in the City of Seattle. In this research, parties affected by municipal practices expressed their hopes and concerns for open data. City personnel from eight prominent

http://btlj.org/
Roadmap

• **Level setting**
• High level regulatory principles and approaches
Level setting

• SF is an exciting, innovative city and I love it!
• This is not an anti-technology talk
• But consider these problems:
  • Innovation often involves experimenting on citizens; the City may be left with the consequences
  • Ideologies of tech leaders may conflict with public values, be perverse, under-conceptualized, out of step
  • Private incentives may conflict with public good
  • Technology shifts balance of power in subtle, sometimes undetectable ways
  • Some technologies are inherently political (Winner, 1986)
Google CEO Larry Page Wants A Totally Separate World Where Tech Companies Can Conduct Experiments On People

Google CEO Larry Page revealed yesterday a radical vision for a semi-lawless utopia where technologists could experiment with society.

Page was speaking at I/O, Google's big conference for developers. He took questions from the audience after Google execs delivered a three hour presentation on new products.
DID UBER STEAL GOOGLE’S INTELLECTUAL PROPERTY?

Silicon Valley was built on job-hopping. But when a leader of Google’s self-driving-car unit joined Uber, Google filed suit. Now the Feds are on the case.

By Charles Duhigg
Page was adamant. According to internal Google e-mails, he ordered executives to “make Anthony rich if Chauffeur succeeds.” Two months later, Google bought 510 Systems for twenty-two million dollars. It also purchased Anthony’s Robots; in return, Levandowski was guaranteed a future payment tied to the total value of Project Chauffeur. Google agreed to give him a claim on ten per cent of the division’s eventual worth—a kind of shadow equity that would vest in four years. The stake eventually paid him more than a hundred and twenty million dollars, one of the largest such payouts in Google’s history.
One day in 2011, a Google executive named Isaac Taylor learned that, while he was on paternity leave, Levandowski had modified the cars’ software so that he could take them on otherwise forbidden routes. A Google executive recalls witnessing Taylor and Levandowski shouting at each other. Levandowski told Taylor that the only way to show him why his approach was necessary was to take a ride together. The men, both still furious, jumped into a self-driving Prius and headed off.

The car went onto a freeway, where it travelled past an on-ramp. According to people with knowledge of events that day, the Prius accidentally boxed in another vehicle, a Camry. A human driver could easily have handled the situation by slowing down and letting the Camry merge into traffic, but Google’s software wasn’t prepared for this scenario. The cars continued speeding down the freeway side by side. The Camry’s driver jerked his car onto the right shoulder. Then, apparently trying to avoid a guardrail, he veered to the left; the Camry pinwheeled across the freeway and into the median.

Levandowski, who was acting as the safety driver, swerved hard to avoid colliding with the Camry, causing Taylor to injure his spine so severely that he eventually required multiple surgeries.
Since 2014, California regulations have required companies to report any instance in which a self-driving vehicle is “in any manner involved in a collision originating from the operation of the autonomous vehicle on a public road that resulted in the damage of property or in bodily injury or death.” The Camry accident occurred three years before this regulation was passed; since the rule went into effect, Google has reported thirty-six additional accidents. If Google is still failing to report accidents in which its cars did not hit other vehicles, then there may have been more undocumented incidents. “There’s lots of times something happened because one of our cars drove erratically but never hit anyone,” a former senior Google executive told me. Google cars sometimes stopped suddenly, including at intersections, causing other cars to swerve. (A spokesperson for Google declined to discuss the company’s reporting policies.)
Our personality traits and political predispositions are predictable from the “likes” we give away free on Facebook

...people’s personalities can be predicted automatically and without involving human social-cognitive skills.
Accuracy (self-other agreement)

Number of Facebook Likes (log scaled)

Michal Kosinski and Yilun Wang, *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images* (2017)

Once Facebook or Google has images of you, your children, your citizens, there is no way to detect or stop its use of face recognition or analysis of medical conditions or personality traits.
Roadmap

- Level setting
- Regulatory principles and approaches
Strategies

• Start by identifying terminal goals
  • Instrumental goals get confused with terminal ones
• Get the engineers in the room (lawyers are good fakers)
• Public choice lens
  • Are data companies “rent seeking” through contracts, regs to create open data
Strategies Con’t

• Incentives are as powerful as law
  • They can be shaped to create deterrence or compellence

• Embrace cost benefit analysis, but keep in mind that it’s mostly used (poorly) as an anti-regulatory tool
  • Must consider non-economic costs: transaction costs, time, etc.

• Can your regulatory approach create/enable a market?
Understanding tech company strategy

• They’re in it for the long game
  • Winner take all

• They have three powerful rhetorical techniques:
  • It’s “free”
    • This is a version of the Bechtel model
  • Trust / the “charm offensive”
    • Replace “Google” with “Raytheon,” would you still hand over the medical database on the same terms?
  • Inevitability
    • Nothing is inevitable

• Industry trade groups echo & magnify their voices, but w/o accountability
Information industry challenges

- Information companies’ products are shapeless & abstract
  - California banned collection of PII at the cash register and so retailers circumvented the ban by asking customers for zip codes and linking zip codes to home address w/ data broker directories. See *Pineda v. Williams-Sonoma Stores, Inc.*, 246 P.3d 612 (SCT Ca. 2011).

- They tell the “truth” and still can be highly misleading, usually by *selective omission* of information uses
  - Uses such as “product improvement” can justify reading your email
Info industry challenges cont.

- Services can blackmail users
- Monitoring undermines users security
- Thus users need public enforcers
I did not expect that every single post I had ever made on Facebook would potentially be rehashed in an interrogatory responses and deposition. At the time I made these posts, I intended for them to be shared with only a limited number of recipients to whom I am connected through Facebook’s social network.
We “never sell your data” but...

• In exchange for getting just a few hundred thousand people to spend more time on Facebook completing surveys, Facebook was willing to give Kogan access to its “Open Graph,” that is, your data and the data of your friends—tens of millions of them.

• Use “sign in with Google” and get user profiles; until recently, Google would allow developers to suck down email inboxes in exchange for developing even trivial webmail plugins

• Main lesson here: companies will promise “not to sell” but accomplish the same outcome using other economic arrangements. Need to define “sale” broadly as any transfer for value
Role of self regulation

• Many upsides: quick, can be expert, avoids legislative tussle
• How to do it well?
  • Start with a clear policy objective (terminal goal)
    • If the industry can’t agree on a healthy terminal goal, the self-regulatory effort will fail
  • Be sure non-industry players participate in the rule setting
  • Self-regulation has to have some kind of legal infrastructure
    • Institutional?
  • Be sure adherents can be held responsible for compliance
    • E.g. FTC considers violating promises as deceptive trade practices
• Self-regulation often happens under the threat of real regulation
Role of “consent”

• Consider both substance and procedure
• Lawyers love to reduce consent to a meaningless procedure

• Substance: would a reasonable person who knows the facts of the plan agree to have their data used in specified ways?

• Procedure: how and when will the person consent? Is it voluntary?
Default choices matter

• In opt-in, the consumer must take some affirmative action to accept a collection or use of data. This places the burden on the business to get permission.
• In opt-out, the consumer must take action to object to data collection or use, thus placing the burden on the consumer to act.
• Product adoption ~= opt-in
• Opt-in: businesses carry costs, can make some models practically impossible
• Basically no one will opt in.
• Opt-in has first amendment problems under *IMS Health*
Designing opt—out fairly

• Opt-out places the burden on the consumer
  • People need to know about the right and they don’t (e.g. bank privacy)
  • Sets up bad incentives: businesses can use transaction costs, framing to stop people from opting out
  • Probably has racial, low-SES implications (see FTC Sunstasia Study by Letzler et al (2004)).

• On the web, you can design mechanisms to require a choice that is neither opt in nor opt out (e.g. use “required” fields, consider Delta.com’s flight insurance model)

• Allow opt outs from third parties (this creates a market for opt out)
Only regulators read notices

• Lawyers love notice but no one can possibly read them, nor it is worthwhile to do so because they are too vague to impart useful information

• Use notices to bind companies to promises; think of the audience as being regulators rather than consumers

• Therefore, look for promises, examples
  • “Would you be willing to put that in your privacy policy?”

• GDPR requires “legitimate interest” uses, “information sharing partners” to be enumerated
Consider legislative “sunsets”

• Sunsets simply cause a rule to “sunset” or expire on some certain date
• Sunsets make you work harder
• However, sunsets can avoid reduce legislative thickets, cause parties to come back to the table when (chances are) the competitive landscape has changed
• One of the best contributions from public choice theory
Consider performance standards

• Credit reporting (CRAs) are regulated by the Federal FCRA

• 1970 Legislative solution was a performance-based standard:
  • CRAs shielded from defamation liability if they adopted techniques to ensure “maximum possible accuracy”
  • Terminal goal: accuracy
  • Instrument: performance standard + procedural rights
  • Ex post approach

HOW THE FAIR CREDIT REPORTING ACT REGULATES BIG DATA

Chris Jay Hoofnagle

INTRODUCTION

This short essay makes two observations concerning “big data.” First, big data is not new. Consumer reporting, a field where information about individuals is aggregated and used to assess credit, tenancy, and employment risks, achieved the status of big data in the 1960s. Second, the Fair Credit Reporting Act of 1970 (FCRA) provides rich lessons concerning possible regulatory approaches for big data.

Some say that “big data” requires policymakers to rethink the very nature of privacy laws. They urge policymakers to shift to an approach where governance focuses upon “the usage of data rather than the data itself.” Consumer reporting shows us that while use-based regulations of big data provided more transparency and due process, they did not create adequate accountability. Indeed, despite the interventions of the FCRA, consumer reporting agencies (CRAs) remain notoriously unresponsive and unaccountable bureaucracies.

Like today’s big data firms, CRAs lacked a direct relationship with the consumer, and this led to a set of predictable pathologies and externalities. CRAs have used messy data and fuzzy logic in ways that produce error costly to consumers. CRAs play a central role in both preventing and causing identity fraud, and have turned this problem into a business opportunity in the form of credit monitoring. Despite the legislative bargain created by the FCRA, which insulated CRAs from defamation suits, CRAs have argued that use restrictions are unconstitutional.

Big data is said to represent a powerful set of technologies. Yet, proposals for its regulation are weaker than the FCRA. Calls for a pure use-based regulatory regime, especially for companies lacking the discipline imposed by a consumer relationship, should be viewed with skepticism.

Performance standards can deal with emergent problems

- Judy Thomas sued TransUnion for regularly mixing her report with a Judith Upton.
- Thomas’ SSN was on digit different from Upton’s + they shared “Jud” in the first name
- CRAs expert systems classified women by their first names!

Los Angeles Times

Jury Awards $5.3 Million for Credit Report Errors
July 31, 2002 | KATHY M. KRISTOF | TIMES STAFF WRITER

An Oregon woman who fought for six years to clear erroneous items from her credit report was awarded $5.3 million Monday by a federal jury in Oregon.

The verdict against Chicago-based credit reporting firm Trans Union was the largest amount ever awarded for violations of the Fair Credit Reporting Act, which requires credit reporting companies to keep accurate records and promptly correct mistakes, consumer attorneys said Tuesday.
Thank you

choofnagle@Berkeley.edu