A Contextual Approach to Privacy: Theory and Application

Helen Nissenbaum
New York University

Institut Mines-Télécom

Paris 10.15.13

Research supported by US-AFSOR: ONR BAA 07-03 (MURI), US NSF CT-M: Privacy, Compliance, & Information Risk CNS-0831124, & Intel Science and Technology Center for Social Computing

Why privacy? Why now?

TECHNOLOGY AND PRIVACY

GPS, mobile, implantable devices

RFID, “emanations”

Biometrics

Pervasive sensory networks

Networked video and audio capture

Web cookies, flash cookies, web bugs

Databases, storage, retrieval

Information aggregation, mining, profiling

“Big data,” “data science, ‘ …

The Internet, the Web

Social computing, Web 2.0

Email, mobile media

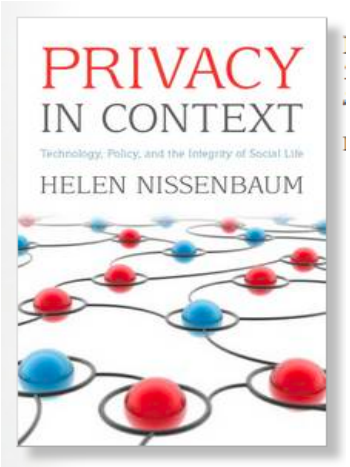
Sociotechnical systems

What makes them privacy threats?

How is privacy protected?

- Diminished Control
  - Control returned
- Increased exposure
  - Increased secrecy
- Private/public dichotomy breached
  - Protect privacy of private

Contextual Integrity



Respecting privacy

does **not** mean …

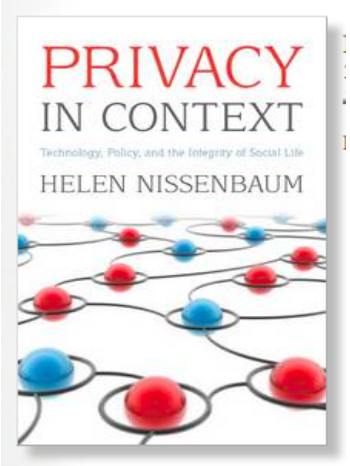
- subject controls data!
- data flow is stopped (secrecy)!
- no flow in private zone (and inverse)

it **does** mean …

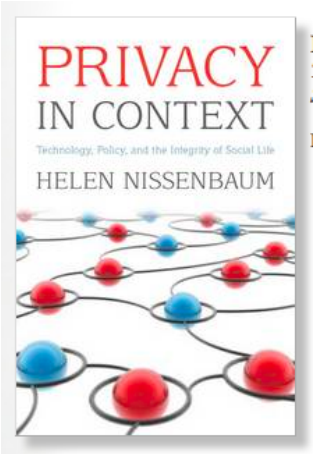
- appropriate flow/sharing
- appropriate constraints

Contextual Integrity shifts privacy question

What is appropriate flow??



Privacy as Contextual Integrity: Key Concepts



Contexts

Structured social spheres defined by activities, practices, roles, … e.g. healthcare, education, social & home-life, professional & work-life, commercial marketplace (e.g. Pierre Bourdieu)

Informational Norms

Context specific rules, customs, conventions, expectations, laws, defining appropriate flows of personal information

Purposes and values

General ethical and political + context specific ends, purposes and values

Informational norms model Appropriate Flow

In a job interview, the interviewer asks about a candidate's past work experience but not about religious observance

A priest never shares congregants' confessions with others

A citizen of the U.S. reveals gross income to the IRS, under strict conditions of confidentiality except as required by law

You do not share a friend's secrets with others, except, perhaps, with your spouse, unless your friend expressly requests otherwise

Parents closely monitor their children's academic performance

Informational norms: Key Parameters

Actors
Sender
Recipient
Subject

Physician, merchant, bank, friend
Merchant, police, ad network
Patient, shopper, investor, reader

Information types

Demographic, biographical
Transactional, communications
Medical status, financial

Transmission Principles

Consent, coerce, steal, buy, sell
Confidentially, stewardship
With a warrant, surreptitiously
[An indefinitely large domain]

Privacy as Contextual Integrity: Key Concepts

Appropriate flows/constraints modeled by Context-specific Informational norms

<Information Type/Attributes> about <Data Subject> is transmitted from <Sender> to <Recipient> under <conditions defined by Transmission Principle>

Actors; Attributes; Transmission Principles

Ideal norms promote values and purposes

Respecting Privacy means …

Respecting **entrenched context specific** informational norms

Respecting Privacy means …

Respecting **entrenched context specific** informational norms

This is a terribly conservative theory!

Evaluating disruption: how?

- Interests
- General moral, social, and political values
- Internal context-specific ends, purposes and values

Considerations

- Interests – often conflicted
  - Informational harms, benefits, risks
  - Boundary control (Altman)
- General moral, social, and political rights & values
  - Unfair discrimination …
  - Liberty, autonomy …

Considerations

Context specific purposes and values

- healthcare: cure disease; alleviate suffering, equity …
- political: democracy; freedom from exploitation …
- home and social: trust, autonomy, stability …
- education: knowledge, intellect, fair distribution

"While the government does not know every source of income of a taxpayer and must rely upon the good faith of those reporting income, still in the great majority of cases this reliance is entirely justifiable, principally because the taxpayer knows that in making a truthful disclosure of the sources of his income, information stops with the government. It is like confiding in one's lawyer."

Secretary of the Treasury, Andrew Mellon, 1925

Respecting Privacy means

- Respecting **entrenched context specific** informational norms
- Accepting disruptive flows in place of entrenched i-norms only if:
  - Interests are balanced
  - general rights & values respected
  - context specific ends, purposes, values sustained

Note:

Privacy is not the opposite of sharing; it is the opposite of inappropriate sharing

Information is not yours, it is about you

The contours of privacy are socially (culturally) varied

Letting people choose may be neither in their interest nor morally required

Feb 23, 2012

White House announces Privacy Bill of Rights

Applications

"where the rubber hits the road"

1. Test CI
2. Utilize

Diagnostic + Prescriptive

Applications:
Empirical + Analytical + Technical

- ✧ Disruptive flows?
- ✧ Locate nature and sources of disruption
- ✧ Evaluate disruptions [not all change is good/bad]
  - ✧ Interests
  - ✧ general ethical and political values
  - ✧ context specific ends, purposes, values

Applications - Empirical

- eCommerce (Kirsten Martin)
- **Placement of Court Records Online [RECAP study]**
- **Health IT and Privacy [SHARPS]**
  - **Anupam Datta, et. al.**
  - Martin French, Heather Patterson: cardio patients expectations in mobile health tracking [Northwestern, UC Berkeley, NYU collaboration]
  - Heather Patterson: Mobile Apps (e.g. Fitbit) and user expectations

Oakland 2006: LPU

$$\sigma \models \Box \forall p_1, p_2, q : P. \forall m : M. \forall t : T.$$

$$\text{incontext}(p_1, c) \wedge \text{send}(p_1, p_2, m) \wedge \text{contains}(m, q, t) \rightarrow \bigvee_{\varphi^+ \in \text{norms}^+(c)} \varphi^+ \wedge \bigwedge_{\varphi^- \in \text{norms}^-(c)} \varphi^- \quad (1)$$

positive norm: $\text{inrole}(p_1, \hat{r}_1) \wedge \text{inrole}(p_2, \hat{r}_2) \wedge \text{inrole}(q, \hat{r}) \wedge (t \in \hat{t}) \wedge \theta \wedge \psi$

negative norm: $\text{inrole}(p_1, \hat{r}_1) \wedge \text{inrole}(p_2, \hat{r}_2) \wedge \text{inrole}(q, \hat{r}) \wedge (t \in \hat{t}) \wedge \theta \rightarrow \psi$

Figure 1. Norms of Transmission Represented as a Temporal Formula

From: A. Barth, A. Datta, J. Mitchell, and H. Nissenbaum, "Privacy and Contextual Integrity: Framework and Applications," Proceedings of the IEEE Symposium on Security and Privacy, May 2006.

HIPAA excerpt

SHARPS

A covered entity may disclose an individual's protected health information (phi) to law-enforcement officials for the purpose of identifying an individual if the individual made a statement admitting participating in a violent crime that the covered entity believes may have caused serious physical harm to the victim

- 4.5 §164.510 A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section.
- *[[To whom?]]*

Applications - Analytical

- Placement of court records on open Web
- Online Privacy
- "Respect for Context," what it is and isn't
- Privacy trouble with MOOCs
- Contextual expectations of privacy
  - Andrew Selbst – 4th Amendment
- Health IT and Privacy
  - Martin French: Privacy rules for HIEs [Working with the IL-HIE]

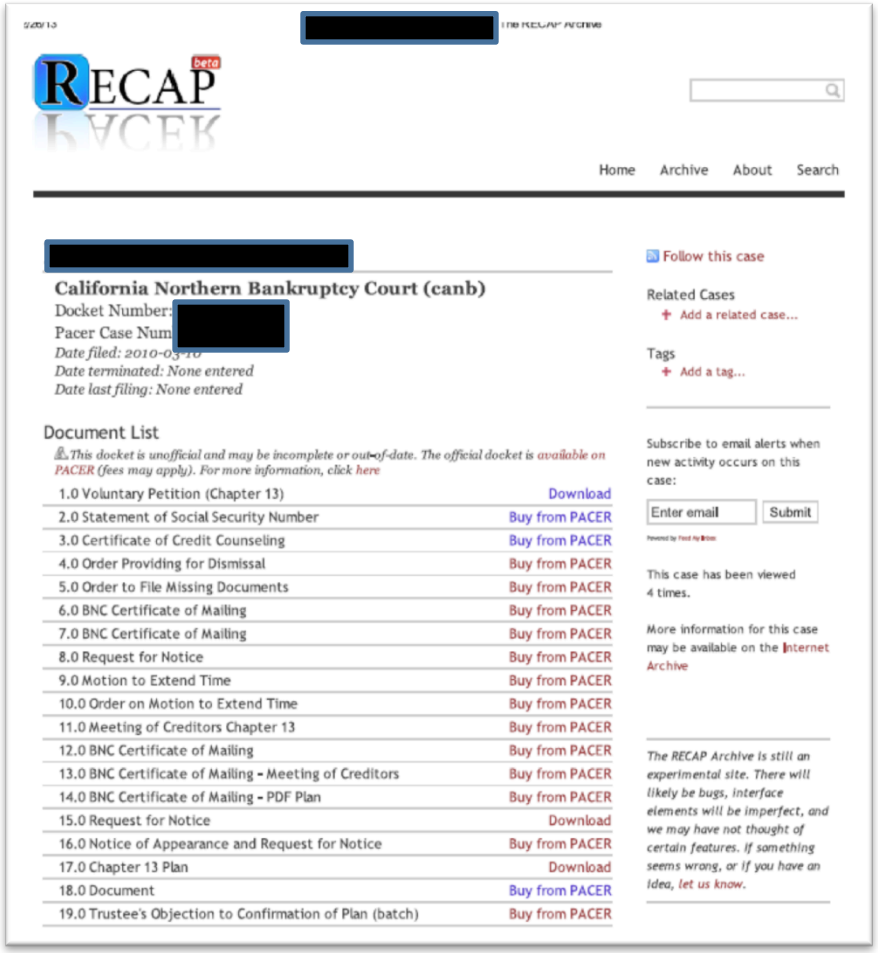
Contextual Integrity as applied to Court Records

- Previous work detailed how contextual integrity (CI) illuminates this shift.
  - Amanda Conley, Anupam Datta, Helen Nissenbaum, and Divya Sharma, *Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry*, 71 Md. L. Rev. 772 (2012).
  - Empirical study that searched for federal electronic records, New Jersey state court records

Bankruptcy Court Records: The old days

Source: United States Bankruptcy Court, Northern District of California, San Jose Division, http://www.canb.uscourts.gov/court-information/locations/san-jose-division

Case Study: RECAP



RECAP beta

Home Archive About Search

California Northern Bankruptcy Court (canb)

Docket Number:

Pacer Case Num

Date filed: 2010-05-10

Date terminated: None entered

Date last filing: None entered

Follow this case

Related Cases

+ Add a related case...

Tags

+ Add a tag...

Subscribe to email alerts when new activity occurs on this case:

Enter email Submit

This case has been viewed 4 times.

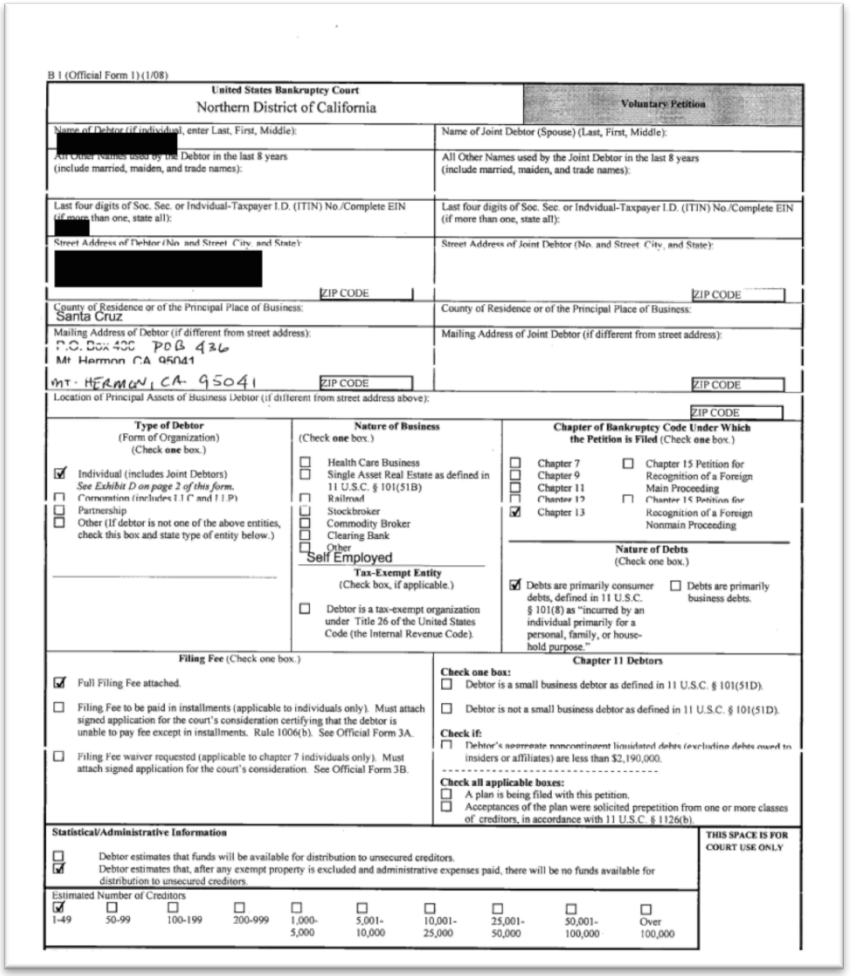
More information for this case may be available on the Internet Archive

The RECAP Archive is still an experimental site. There will likely be bugs, interface elements will be imperfect, and we may have not thought of certain features. If something seems wrong, or if you have an idea, let us know.

Document List

This docket is unofficial and may be incomplete or out-of-date. The official docket is available on PACER (fees may apply). For more information, click here

1.0 Voluntary Petition (Chapter 13)	Download
2.0 Statement of Social Security Number	Buy from PACER
3.0 Certificate of Credit Counseling	Buy from PACER
4.0 Order Providing for Dismissal	Buy from PACER
5.0 Order to File Missing Documents	Buy from PACER
6.0 BNC Certificate of Mailing	Buy from PACER
7.0 BNC Certificate of Mailing	Buy from PACER
8.0 Request for Notice	Buy from PACER
9.0 Motion to Extend Time	Buy from PACER
10.0 Order on Motion to Extend Time	Buy from PACER
11.0 Meeting of Creditors Chapter 13	Buy from PACER
12.0 BNC Certificate of Mailing	Buy from PACER
13.0 BNC Certificate of Mailing - Meeting of Creditors	Buy from PACER
14.0 BNC Certificate of Mailing - PDF Plan	Buy from PACER
15.0 Request for Notice	Download
16.0 Notice of Appearance and Request for Notice	Buy from PACER
17.0 Chapter 13 Plan	Download
18.0 Document	Buy from PACER
19.0 Trustee's Objection to Confirmation of Plan (batch)	Buy from PACER



B 1 (Official Form 1) (1/08)

United States Bankruptcy Court
Northern District of California

Voluntary Petition

Name of Debtor (if individual, enter Last, First, Middle):

Name of Joint Debtor (Spouse) (Last, First, Middle):

All Other Names used by the Debtor in the last 8 years (include married, maiden, and trade names):

All Other Names used by the Joint Debtor in the last 8 years (include married, maiden, and trade names):

Last four digits of Soc. Sec. or Individual-Taxpayer I.D. (ITIN) No./Complete EIN (if more than one, state all):

Last four digits of Soc. Sec. or Individual-Taxpayer I.D. (ITIN) No./Complete EIN (if more than one, state all):

Street Address of Debtor (No. and Street, City, and State):

ZIP CODE

Street Address of Joint Debtor (No. and Street, City, and State):

ZIP CODE

County of Residence or of the Principal Place of Business: Santa Cruz

County of Residence or of the Principal Place of Business:

Mailing Address of Debtor (if different from street address): P.O. Box 436 PDB 436 Mt. Hermon CA 95041

Mt. Hermon, CA 95041 ZIP CODE

Mailing Address of Joint Debtor (if different from street address):

ZIP CODE

Location of Principal Assets of Business Debtor (if different from street address above):

ZIP CODE

Type of Debtor (Form of Organization) (Check one box.)

- [x] Individual (includes Joint Debtors) *See Exhibit D on page 2 of this form.*
- [ ] Corporation (includes LLC and LLP)
- [ ] Partnership
- [ ] Other (If debtor is not one of the above entities, check this box and state type of entity below.)

Nature of Business (Check one box.)

- [ ] Health Care Business
- [ ] Single Asset Real Estate as defined in 11 U.S.C. § 101(51B)
- [ ] Railroad
- [ ] Stockbroker
- [ ] Commodity Broker
- [ ] Clearing Bank
- [ ] Other

Self Employed

Tax-Exempt Entity (Check box, if applicable.)

- [ ] Debtor is a tax-exempt organization under Title 26 of the United States Code (the Internal Revenue Code).

Chapter of Bankruptcy Code Under Which the Petition is Filed (Check one box.)

- [ ] Chapter 7
- [ ] Chapter 9
- [ ] Chapter 11
- [ ] Chapter 12
- [x] Chapter 13
- [ ] Chapter 15 Petition for Recognition of a Foreign Main Proceeding
- [ ] Chapter 15 Petition for Recognition of a Foreign Nonmain Proceeding

Nature of Debts (Check one box.)

- [x] Debts are primarily consumer debts, defined in 11 U.S.C. § 101(8) as "incurred by an individual primarily for a personal, family, or household purpose."
- [ ] Debts are primarily business debts.

Filing Fee (Check one box.)

- [x] Full Filing Fee attached.
- [ ] Filing Fee to be paid in installments (applicable to individuals only). Must attach signed application for the court's consideration certifying that the debtor is unable to pay fee except in installments. Rule 1006(b). See Official Form 3A.
- [ ] Filing Fee waiver requested (applicable to chapter 7 individuals only). Must attach signed application for the court's consideration. See Official Form 3B.

Chapter 11 Debtors

Check one box:

- [ ] Debtor is a small business debtor as defined in 11 U.S.C. § 101(51D).
- [ ] Debtor is not a small business debtor as defined in 11 U.S.C. § 101(51D).

Check if:

- [ ] Debtor's aggregate noncontingent liquidated debts (excluding debts owed to insiders or affiliates) are less than $2,190,000.

Check all applicable boxes:

- [ ] A plan is being filed with this petition.
- [ ] Acceptances of the plan were solicited prepetition from one or more classes of creditors, in accordance with 11 U.S.C. § 1126(b).

Statistical/Administrative Information

THIS SPACE IS FOR COURT USE ONLY

- [ ] Debtor estimates that funds will be available for distribution to unsecured creditors.
- [x] Debtor estimates that, after any exempt property is excluded and administrative expenses paid, there will be no funds available for distribution to unsecured creditors.

Estimated Number of Creditors

1-49	50-99	100-199	200-999	1,000-5,000	5,001-10,000	10,001-25,000	25,001-50,000	50,001-100,000	Over 100,000
[x]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Contextual Integrity as applied to Court Records

- Previous work detailed how contextual integrity (CI) illuminates this shift.
  - Amanda Conley, Anupam Datta, Helen Nissenbaum, and Divya Sharma, *Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry*, 71 Md. L. Rev. 772 (2012).
  - Empirical study that searched for federal electronic records, New Jersey state court records

Contextual Integrity as applied to Court Records

- Findings:
  - Different cost of flows of personal information between online and local access systems, based on:
    - Location of information system
    - Query interface and indexing mechanism
    - Linked information sources
    - Access restrictions
    - Record format
    - Human factors

Possible models to guide information flow

- “Fine-grained differential access”
  - Vary access based on, for example,
    - the roles of parties requesting access
    - the roles of information subjects
    - the types of information, and
    - the conditions under which information is granted.

IV. Work-in-progress: Tailored Rules for Privacy and Transparency?

NEW YORK UNIVERSITY

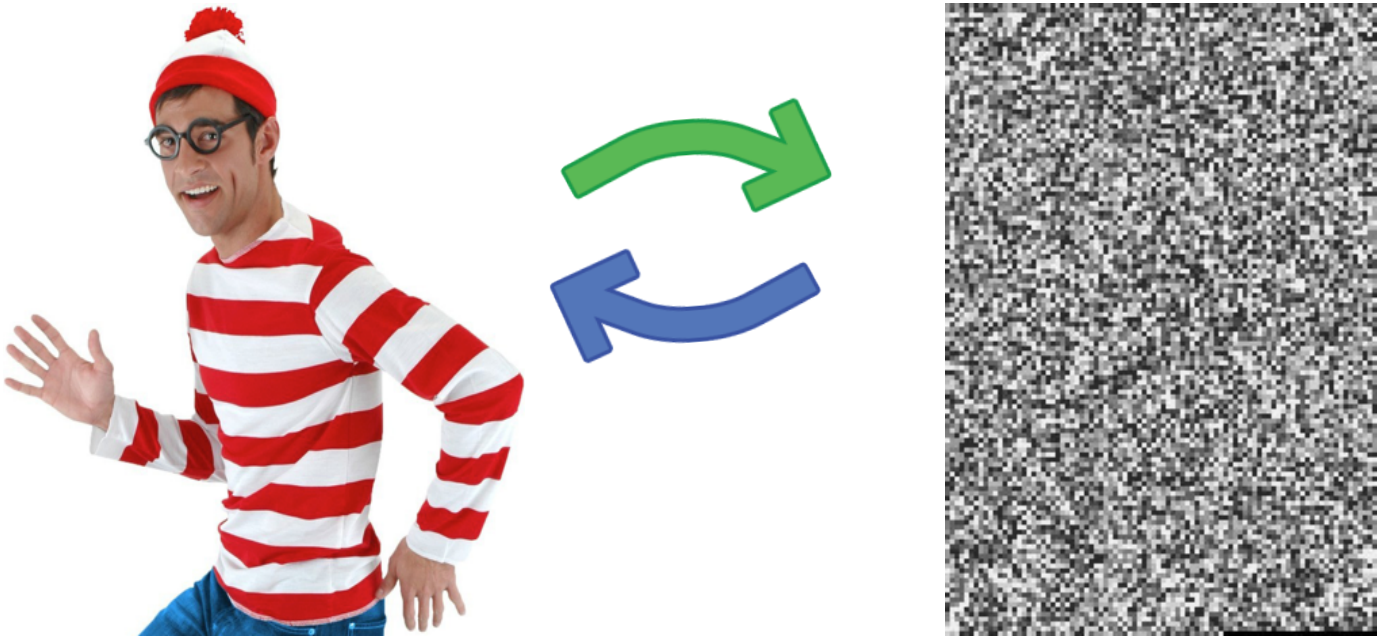
Applications - Technical

- Context-Aware DNT: FF extension
  - automatically sets DNT header based on page content, using *Adnostic* ontology
- **Cryptagram: privacy for photo sharing**
- Compass
- **Obfuscation**
  - **TrackMeNot (with V. Toubiana and D. Howe)**
  - **"AdNauseum" (with D. Howe)**

Cryptagram

photo privacy for online social media

http://cryptagr.am



- Appropriate photo access and control
- Stops server side gleaning and facial recognition
- Retains key photo sharing experience

Matt Tierney, Ian Spiro, Chris Bregler, Lakshmi Subramanian | PRGLab | NSF IGERT

OBFUSCATION: OUR DEFINITION

"The production, inclusion, addition, or communication of misleading, ambiguous , or false data in an effort to evade, distract, or confuse data gatherers or diminish the reliability (and value) of data aggregations."

[Brunton, Nissenbaum] "Vernacular resistance to data collection and analysis: A political philosophy of obfuscation," *First Monday*, May 2011

?

From “A Plausible Thought About the Future: Safeguarding Privacy with Deception, by Conor Friedersdorf, The Atlantic, 9/19/2011

"It took me back to Buffalo, to the pignoli, a Sicilian version of macarons studded with pine nuts that my Aunt Lili made in huge batches at Christmas.

… she kept her recipe secret, not by withholding it, but by slightly altering proportions of the ingredients in every retelling."

Elaine Sciolino, "Fads Aside, the Perfect Macaron is timeless" *The New York Times*, July 22, 2013

TrackMeNot

Version 0.8.3

Created by: Daniel C. Howe (@danielchowe), Helen Nissenbaum (@HNissenbaum)
Maintained by: Vincent Toubiana (@vtoubiana)
Homepage: www.cs.nyu.edu/trackmenot/
Translations: Jens 'woelfchen'(German), Tommy Mejldal(Danish),markh van BabelZilla.org(Dutch), rlicul(Croatian), BruceH(Chinese), Edgard Dias Magalhães(Portuguese)

TrackMeNot Options

Help/FAQ | Main Site | Show Queries

- [x] Enabled
- [ ] Use tab to search
- [ ] Enable Query Bursts

Search Engines

Selection

- [x] Google Search –
- [x] Yahoo! Search –
- [x] Bing Search –
- [ ] Baidu Search –
- [ ] Aol Search –

+

To add the engine url, search 'trackmenot' (without the quotes) in the engine you want to add, and copy/past the search url in the URL text box bellow.

Name | URL | Add Engine

Avg. Query Rate:

Query Frequency: 5 per min

Logging Options

- [ ] Disabled
- [x] Persiste

Show Log | Clear Log

RSS Feed

Validate | http://www.nytimes.com/services/xml/rss/nyt/HomePage.xml | p://rss.cnn.com/rss/cnr

Black List

- [x] Use list: bomb,porn,pornographie
- [ ] Generate queries including keywords monitored by DHS

2006 - ongoing

obfuscating web search

[AdNauseum]

Created by: Daniel C. Howe, Helen Nissenbaum

Download [AdNauseum] for Firefox

Background

[AdNauseum] is a lightweight browser extension that helps protect users against surveillance and data-profiling by online advertisers and ad networks. It does so not by means of concealment and encryption (i.e. covering one's tracks), but instead, paradoxically, by the opposite strategy: noise and obfuscation. [AdNauseum] works silently in the background of your web browser by clicking all the ads on a page, thereby obscuring user interests in a cloud of decoy clicks. In light of the industry's failure to achieve consensus on a Do Not Track standard, [AdNauseum] allows individual users to take matters into their own hands, offering cover against certain forms of surveillance, profiling, and practices of discrimination.

For the past 1.5 years W3C has led an effort which has engaged NGOs, industry reps from advertising and tech attempting to achieve a consensus on a standard for Do Not Track (DNT). From several trusted sources, the ad industry continuously sabotages progress, often at the 11th hour, so much so that at least