Ethics Issues for Web Search

What’s the Problem?

• Privacy
  – Query
  – Pages clicked
  – Profiles

• Inappropriate search results
  – Children
  – “Picking” what you want people to see
  – Racial/Gender/Ethnic/… bias
What is Privacy?

• “The right to be let alone” - Warren & Brandeis, 4 Harvard L.R. 193 (Dec. 15, 1890)
  – My information protected so it doesn’t adversely affect me in the future
• Control over data
  – My information used only in ways I approve
• Issues:
  – Disclosure / sharing
  – Approved use
  – Recourse

Data Privacy: The Goal

• Protect the Individual
  – “Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.” – Charter of Fundamental Rights of the European Union

• Challenges: What do we mean by
  – “concerning” an individual
  – Protection
  – Consent
  – Access / rectified
“Obvious” answers

- Concerning an individual
  - Has your name/address/other identifying information
- Protection
  - Only used/accessed in expected, intended, authorized ways
- Consent
  - You know and agree to what is done with the data
- Access/Rectify
  - You can see the data and correct errors

Consent?

The Guardian
Maev Kennedy
Thu 11 Jun 2009 07.17 EDT
American family's web photo ends up as Czech advertisement
Smiths from Missouri only heard about it when a friend travelling in Prague saw them on a grocery store poster
Did they consent to this?

**Facebook didn’t authorize it, it but could they?**

Facebook Terms of Service 4/19/18: when you share, post, or upload content that is covered by intellectual property rights (like photos or videos) on or in connection with our Products, you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings). This means you give us permission to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings). This means you give us permission to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings). This means you give us permission to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings). This means you give us permission to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings).

Before 4/19/18, if shared with others, deleting your account didn’t terminate these rights.

“Obvious” answers

- **Concerning an individual**
  - Has your name/address/other identifying information

- **Protection**
  - Only used/accessed in expected, intended, authorized ways

- **Consent**
  - You know and agree to what is done with the data

- **Access/Rectify**
  - You can see the data and correct errors
Sec. 10. "Personal information" means:

(1) a Social Security number that is not encrypted or redacted; or
(2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:
   (A) A driver's license number.
   (B) A state identification card number.
   (C) A credit card number.
   (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person’s account.

The AOL Awakening

- In Aug 2006, AOL released its customers web searches for research studies
- 20 Million unique queries of 650K unique users
- <user-id> was replaced with a <random number>
- NY Times reporter successfully found the identity of an individual from the queries
  - Queries included “60 single men” “landscapers in Lilburn, Ga”
  - Many more queries contained enough information to uniquely identify the person
- And it keeps going (Netflix, NYC Taxi, …)

AOL fired its CTO over this issue;
Two researchers were forced out
Re-identifying “anonymous” data (Sweeney ’01)

- 37 US states mandate collection of information
- Dr. Sweeney purchased the voter registration list for Cambridge Massachusetts – 54,805 people
- 69% unique on postal code and birth date
- 87% US-wide with all three

Solution: k-anonymity
- Any combination of values appears at least k times
- Developed systems that guarantee k-anonymity
  - Minimize distortion of results

Redaction:

IC 24-4.9-2-11

(a) Data are redacted for purposes of this article if the data have been altered or truncated so that not more than the last four (4) digits of:

(1) a driver's license number;
(2) a state identification number; or
(3) an account number;

is accessible as part of personal information.

(b) For purposes of this article, personal information is "redacted" if the personal information has been altered or truncated so that not more than five (5) digits of a Social Security number are accessible as part of personal information.
Anonymity: The Goal

- Prevent Disclosure of Personal Information
  - GDPR: ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly
  - Qatar Law 13 of 2016: Personal Data: Data belonging to an Individual with specified or reasonably specifiable identity whether through such Personal Data or through combining the same with any other data
  - But still use the data where appropriate!

- Problem: It can’t be done!
  - “Perfect” privacy requires zero utility (e.g., the data must be encrypted.)
  - As soon as we can use the data (e.g., decrypt), it is at risk

Why Perfect Privacy is Impossible
(Dwork, McSherry, Nissim, and Smith ‘06)

- Background Knowledge
  - Adversary may already know a lot
  - Whatever we provide (even de-identified or anonymized data) may add to that knowledge

- It may just take that “last bit of knowledge” to give the adversary the ability to violate privacy
  - We can formally prove 1 bit may be too much
What We Can Do

• Encryption
  – Reduce risk to minimal levels when data not in use
• Anonymization
  – Produce usable data that is hard to link to individuals
• Noise addition
  – Usable data where any link to individuals (or information we surmise about individuals) is guaranteed to be uncertain/suspect

Myth: Anonymity is Broken

• Many academic papers with attacks on anonymization
  – E.g., deFinetti (Kifer’09), Minimality (Wong, Fu, Wang, Pei ’07)
  – Real-world failures (e.g., AOL)
• Reality: There is a risk
  – But risk may be acceptable (e.g., HIPAA safe-harbor rules do not eliminate risk of re-identification)
  – Differential Privacy provides provable limits on risk
  – **Any disclosure that provides utility also carries some privacy risk** (Dwork’06)
Myth: Anonymized Data Isn’t Useful

• Differential Privacy: Noise added for privacy is often small relative to other sources of noise in the data
  – Can even improve statistical value of results (Dwork et al. ‘17)
• Machine Learning models learned from Anonymized Data can be as good or better than using the original data
  – Decision trees on k-anonymous data (Iyengar’02)
  – Support Vector Machines on anatomized data (Mancuhan&Clifton’17)
  – Nearest Neighbor on anonymized data

Use Cases for Anonymity

• Public release
  – Challenging, given possible attacks on anonymity
• Protection from “accidental re-identification”
  – Ethical researchers could see their neighbor…
  – Model: HIPAA Limited Dataset
    • Easily re-identifiable, but only released under Data Use Agreement
• Reduce risk from data breach
  – Which would you rather have stolen, identifiable data or anonymized, possibly re-identifiable data
  – Won’t trigger many breach disclosure laws

  Can still obtain high quality analysis outcomes
What We Need: Legal Incentives

• “Notice and Consent” framework discourages application of technological advances
  – We can’t guarantee your privacy, so please allow us to use your data in unsafe ways
  – U.S.: Enforcement action against Snapchat for promising to protect privacy and not doing a good enough job
    • Companies get away with not even trying, as long as they tell you so
• Can legal frameworks acknowledge that privacy is at risk?
  – Require efforts to manage, not eliminate, that risk

Fair Information Practices

1. Notice/Awareness
2. Choice/Consent
3. Access/Participation
4. Integrity/Security
5. Enforcement/Redress
  – Self-Regulation
  – Private Remedies
  – Government Enforcement

http://www.ftc.gov/reports/privacy3/fairinfo.shtm