

Social Contact In The Time of Tech

Lawrence Snyder
University of Washington, Seattle

Interacting On The WWW

- “Hello, World” – it’s the **WORLD** Wide Web
- Mostly we think of our small circle of friends & organizations when we’re online ... but really the whole world has access
- And, to some degree, we’re anonymous
- So ... we can behave however we like, right?

Interacting On The WWW

- “Hello, World” – it’s the **WORLD** Wide Web
- Mostly we think of our small circle of friends & organizations when we’re online ... but really the whole world has access
- And, to some degree, we’re anonymous
- So ... we can behave however we like, right?

NOT

“Offensensitivity”

- A good guideline for online behavior is www.css-discuss.org/policies.html#offensensitivity
- Key points – when writing online discussion
 - Thousands of people will see it
 - You can easily and unintentionally offend them
 - They can easily and unintentionally offend you
 - The collision comes from different cultures, social norms, backgrounds, assumptions, religions ...
 - You’re not wrong; they’re not wrong ... just different
 - They’re no more likely to change their thinking than you
- Tolerance, open-mindedness, respect needed

Privacy: Tech Changes the Game

■ Justice Louis Brandeis

*The narrower doctrine [of illegal search] may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that **modern devices** afford abundant opportunities for the perpetration of such wrongs without any participation of the injured party, the protection granted by the law must be placed upon a broader foundation.*

What it means if you are not a Supreme Court Justice –

- In the past privacy – protected by 4th Amendment – couldn't be violated for careful people
- Technology has changed all that
- Now it is possible to violate people's privacy without their knowing it

Privacy: Tech Changes the Game

■ Justice Louis Brandeis

*The narrower doctrine [of illegal search] may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that **modern devices** afford abundant opportunities for the perpetration of such wrongs without any participation of the injured party, the protection granted by the law must be placed upon a broader foundation.*

What it means if you are not a Supreme Court Justice –

- In the past privacy – protected by 4th Amendment – couldn't be violated for careful people
- Technology has changed all that
- Now it is possible to violate people's privacy without their knowing it **1890**

Privacy: A Definition

- **Privacy:** *The right of people to choose freely under what circumstances and to what extent they will reveal themselves, their attitude, and their behavior to others.*
 - It's a human right – explicit in many countries
 - **You choose** to do the revealing, no one else
 - You can't live like a hermit; you must reveal
 - With strong privacy protections – the US has almost none – it's OK to reveal, because the receivers of the information must keep it private

Privacy: A Definition

- **Privacy:** *The right of people to choose freely under what circumstances and to what extent they will reveal themselves, their attitude, and their behavior to others.*
 - It's a human right – explicit in many countries
 - **You choose** to do the revealing, no one else
 - You can't live like a hermit; you must reveal
 - With strong privacy protections – the US has almost none – it's OK to reveal, because the receivers of the information must keep it private

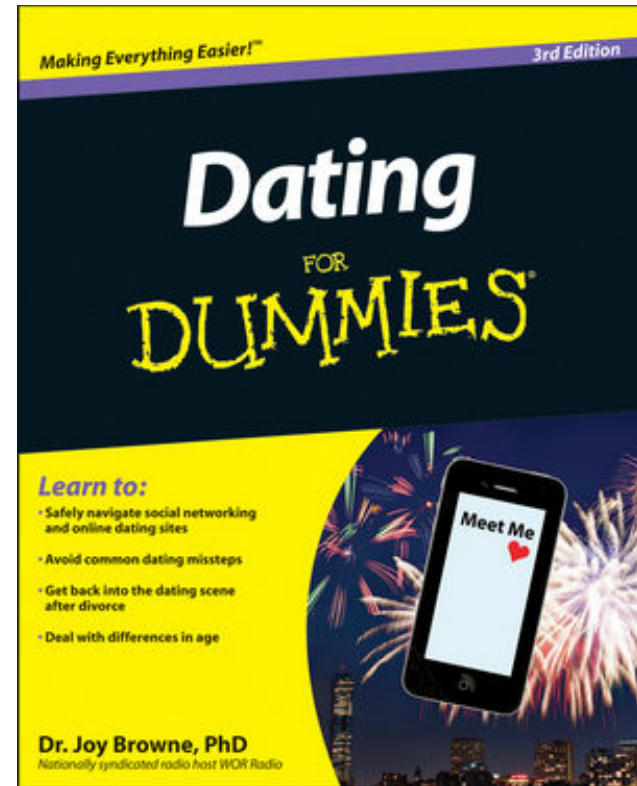
You Produce Information Regularly

- A business transaction ... creates information
 - Date, Time, Store, Cashier, Product, Price, Other stuff in “market basket,” ... can it be connected to you?
 - Pay by cash ... not so likely
 - Pay by credit/debit card, give frequent customer number, apply for warranty coverage, etc.

**Whose Information Is It and
What Happens To It?**

You Produce Information Regularly

- A business transaction ... creates information
If its socks, who cares ... other products are more sensitive



The Information From Purchase

- You and the store seem to be the rightful owners of the information
- How could it be used?
 - No uses – store keeps it only to insure it's paid
 - Opt IN – store uses it only if you approve, say for further business activities involving you
 - Opt OUT – store can use the data however it wants unless you object
 - No limits – any use of the data is fine including identity theft



Are You Pregnant?

- Target data mines customers and can figure out the likelihood a woman is pregnant [NYT]



Are You Pregnant?

- Target data mines customers and can figure out the likelihood a woman is pregnant [NYT]
- The Wonders of Frequent Buyers Cards
 - 25 “key products”
 - Ex: more unscented lotion;
 - Ex: more dietary supplements like Fe
 - Ex: large handbag



Right 7 times in 8

Are You Pregnant?

- Target data mines customers and can figure out the likelihood a woman is pregnant [NYT]



What Target discovered fairly quickly is that it creeps people out that the company knows about their pregnancies in advance.

“If we send someone a catalog and say, ‘Congratulations on your first child!’ and they’ve never told us they’re pregnant, that’s going to make some people uncomfortable,” Pole said. “We are very conservative about compliance with all privacy laws. **But even if you’re following the law, you can do things where people get queasy.**”

Fair Information Practices ...

- For our online social problems one thing we cannot blame is the technology ... it's neutral

OECD Fair Information Practices:

- Limited Collection

There should be limits to the personal data collected; data should be collected by fair and lawful means, and with the knowledge and consent of the person whenever possible.

- Purpose

The purposes for collecting personal data should be stated when it is collected; the uses should be limited to those purposes.

- Quality

The data should be relevant to the purpose of collection; it should be accurate, complete, and up-to-date.

Fair Practices (Continued)

- Use Limitation

Personal data should not be disclosed or used for purposes other than stated in the Purpose Principle, except with the consent of the individual or by the authority of law.

- Security

Personal data should be protected by reasonable security measures against risks of disclosure, unauthorized access, misuse, modification, destruction, or loss.

- Openness

There should be general openness of policies and practices about personal data collection, making it possible to know of its existence, kind, and purpose of use, as well as the contact information for the data controller.

- Participation

An individual should be able to (a) determine if the data controller has information about him or her, and (b) discover what it is. If the request is denied, the individual should be allowed to challenge the denial.

- Accountability

The data controller should be accountable for complying with these principles.

Edward Snowden

- Edward Snowden told Americans that the NSA was collecting its phone call metadata ...
- Many Americans thought this was wrong, and felt violated ... what was wrong?
 - **Purpose** was to conduct phone business responsibly
 - **Use limitation** says they can't change purpose w/o your 'yes'
 - NSA changed it's purpose



What Can You Do?

- Lobby for better privacy controls – Most developed nations have **strong** privacy laws
 - EU, CA, AU, HK, NZ, CH, ...
 - The US? Very, very limited, because ...
-
- ALWAYS pay attention to privacy settings

What Do You Reveal? Self-inflicted

- Even though we do the “revealing” we may be wise not to reveal “all”
- People have lost jobs based on FB posts
- The problem FB and Tweeter, etc. are widely accessed
 - Grandmother (a FB user, too!), HR department, etc.
- Because of technical considerations, the info is not likely to go away ... even if you try deleting



The Problem

- When you look for a job, HR will probably check
- When people first meet you (a potential love interest, say), he/she will almost always check you out ... what image do you want to present?
- You're not really anonymous after all

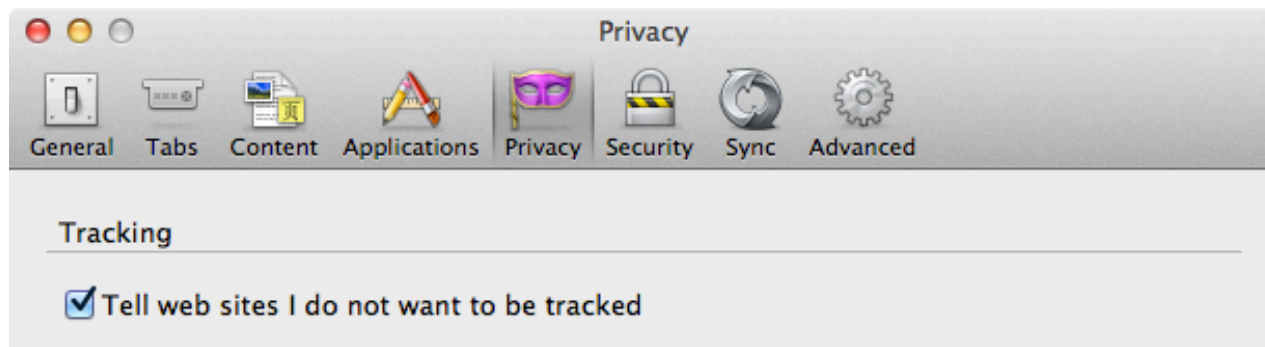
- Guidelines: Watch posts about behavior, schedule, biases, employer, and drama in your life

Guidelines – Think Twice About ...

- Behavior – text or photos on socially unacceptable behavior has cost people jobs
- Schedule – posting or tweeting where you are not – “Off to Hawaii” – is direct help to burglars
- Biases – “hating” others is easy enough to do, but is that how you want your public image?
- The boss may follow your thoughts on your job
- Drama – the drama in our lives often consumes us; it’s hard not to tweet or post about it, but it often reveals information about others

“Do Not Track”

- Tracking means browsers – Chrome, Safari, Internet Explorer, Firefox, ... – send info about your browsing behavior (sites you’re visiting, what you clicked on) back to 3rd parties (marketing, advertising groups, anyone else)
- If that’s OK, do nothing; If that’s not OK –
 - Use Firefox always; avoiding tracking is easy
 - Set “do not track” flag: preferences > security



Copyrights


- Protecting your info is not the only problem
- How you use other people's work is one, too.
- Intellectual property is something produced by one's intellect: art, novels, photos, music, poetry, performances, software, textbooks
- Making a copy of the work for sale or distribution is the right of the creator
 - YOU are the creator of all you create (if not at work)
 - It is illegal to copy someone's creation for "other than personal use"


WWW Makes Copyright Issues Worse


- “Music and videos” are widely stolen
- Most people who have posted to the WWW have probably violated copyright laws
- Owners must “defend” their copyrights, making it a very uncomfortable situation
 - RIAA and MPAA are a war with users
 - Congress, without understanding what it’s doing, nearly passed
 - SOPA – Stop Online Piracy Act
 - PIPA – Protect Intellectual Property Act
- The situation is busted


One Bright Spot

- The Creative Commons allows rights holders to share them while keeping those they want

 **ATTRIBUTION:** Others are allowed to copy, distribute, perform, etc. work, as well as create other work based on it, and you get credit for it.

 **NONCOMMERCIAL:** Others are allowed to copy, distributed, perform, etc. work, as well as create other work based on it, as long as the result is not for sale.

 **NO DERIVATIVE WORK:** Others are allowed to copy, distributed, perform, etc. work, as long as those are verbatim; no derivative works can be created from it.

 **SHARE ALIKE:** Others are allowed to distribute derivative works only under a license identical to the one governing your work.

Summary

- Privacy is a human right. We all deserve it, but in the US it is consistently compromised
- Inform yourself – the EFF (Electronic Freedom Foundation), ALA (American Library Association), and the ACLU (American Civil Liberties Union) are avid defenders of privacy
- Act – a variety of simple changes (do not track) can keep much of your information private