Moral and Legal Foundations of Privacy

February 28, 2023

IV. Privacy in the Digital Age

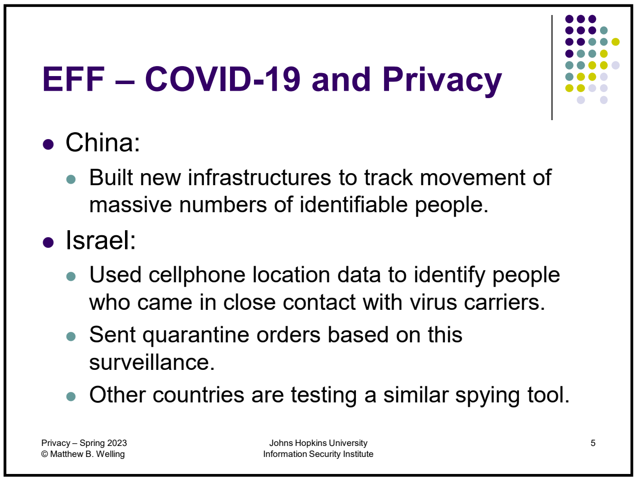
1. Practical Implications

EFF – Governments Haven’t Shown Location Surveillance Would Help Contain COVID-19

COVID-19 and Privacy

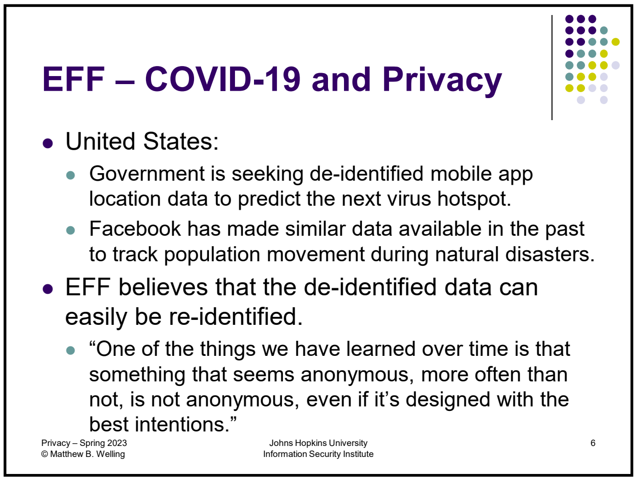
EFF – COVID-19 and Privacy

- March 2020 article from EFF at the beginning of the pandemic in the U.S.
- Article touches on location surveillance and the Fourth Amendment issues discussed in class so far.
- Governments are interested in containing COVID-19, but EFF believes that one measure, location surveillance, violates individual privacy and other rights.



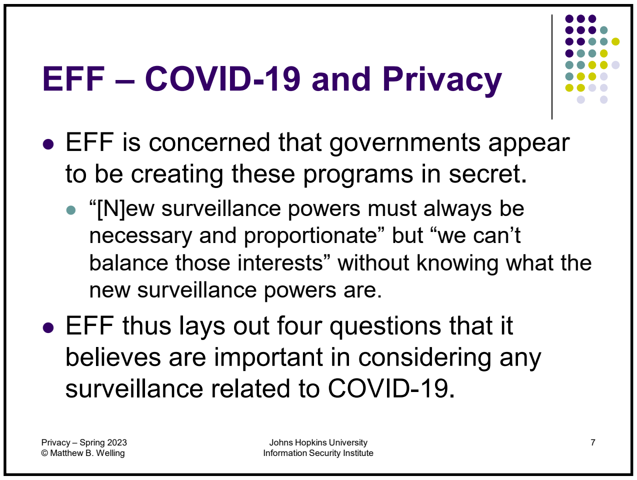
EFF – COVID-19 and Privacy

- China:
  - Built new infrastructures to track movement of massive numbers of identifiable people.
- Israel:
  - Used cellphone location data to identify people who came in close contact with virus carriers.
  - Sent quarantine orders based on this surveillance.
  - Other countries are testing a similar spying tool.



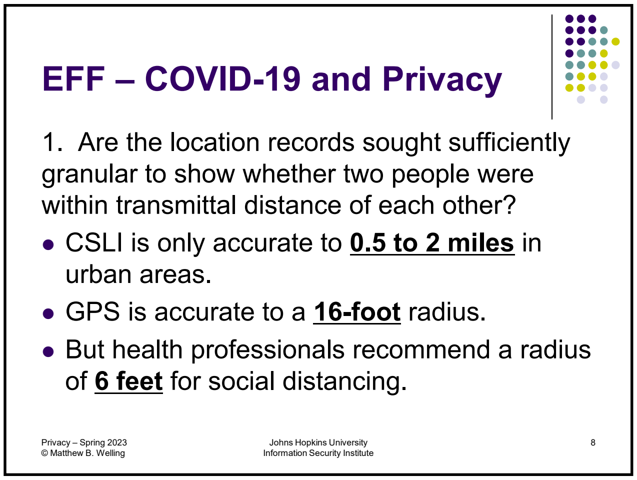
EFF – COVID-19 and Privacy

- United States:
  - Government is seeking de-identified mobile app location data to predict the next virus hotspot.
  - Facebook has made similar data available in the past to track population movement during natural disasters.
- EFF believes that the de-identified data can easily be re-identified.
  - “One of the things we have learned over time is that something that seems anonymous, more often than not, is not anonymous, even if it’s designed with the best intentions.”



EFF – COVID-19 and Privacy

- EFF is concerned that governments appear to be creating these programs in secret.
  - “[N]ew surveillance powers must always be necessary and proportionate” but “we can’t balance those interests” without knowing what the new surveillance powers are.
- EFF thus lays out four questions that it believes are important in considering any surveillance related to COVID-19.



EFF – COVID-19 and Privacy

1. Are the location records sought sufficiently granular to show whether two people were within transmittal distance of each other?

- CSLI is only accurate to **0.5 to 2 miles** in urban areas.
- GPS is accurate to a **16-foot** radius.
- But health professionals recommend a radius of **6 feet** for social distancing.

EFF – COVID-19 and Privacy

2. Do the cellphone location records identify a sufficiently large and representative portion of the overall population?

- Not everybody has a cell phone.
- Older people are at higher risk of COVID-19, but tend not to have cell phones.

EFF – COVID-19 and Privacy

3. Has the virus already spread so broadly that contact tracing is no longer a significant way to reduce transmission?

- Should the government thus divert its resources away from location tracking and toward other containment methods, like widespread testing?

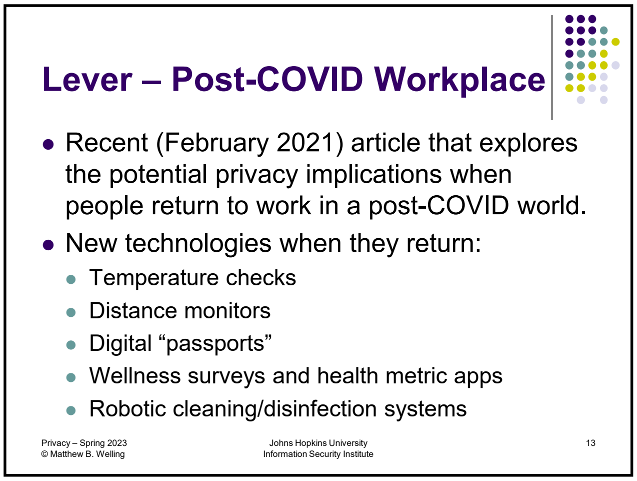
EFF – COVID-19 and Privacy

4. Will health-based surveillance deter people from seeking health care?

- According to the EFF, there are already reports that people subject to COVID-based location tracking are altering their movements to avoid embarrassment.
- If a positive COVID test leads to enhanced location surveillance, some people may avoid getting tested.

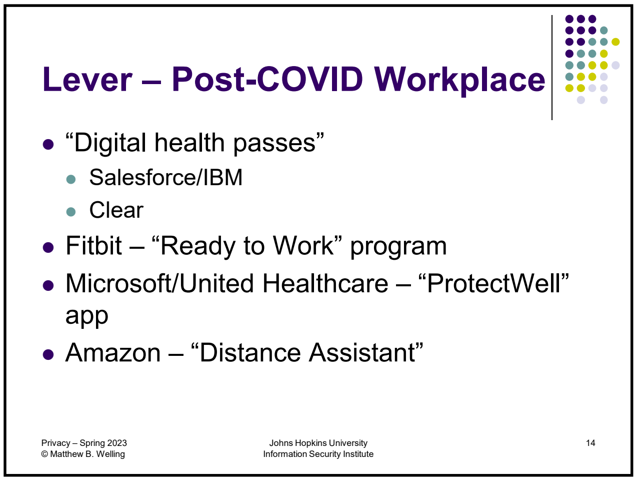
Lever – Privacy Faces Risk in Tech-Infused Post-COVID Workplace

COVID-19 and Privacy



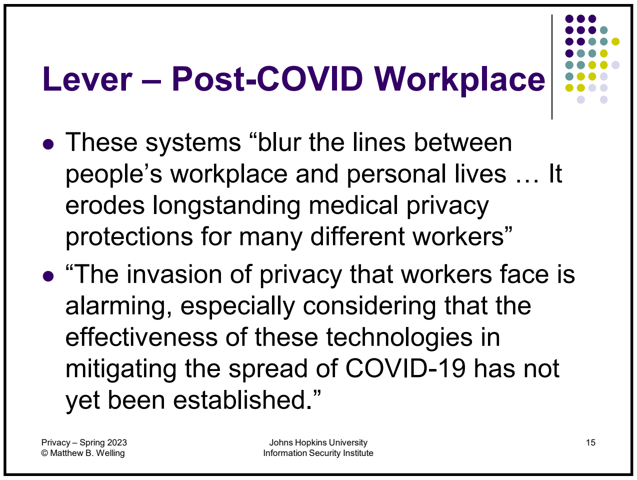
Lever – Post-COVID Workplace

- Recent (February 2021) article that explores the potential privacy implications when people return to work in a post-COVID world.
- New technologies when they return:
  - Temperature checks
  - Distance monitors
  - Digital “passports”
  - Wellness surveys and health metric apps
  - Robotic cleaning/disinfection systems



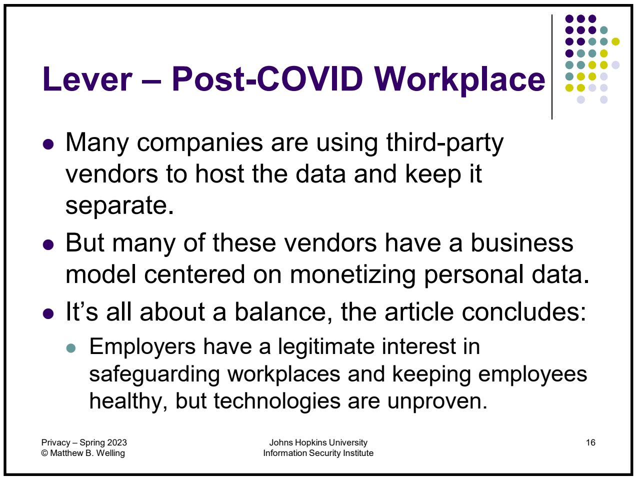
Lever – Post-COVID Workplace

- “Digital health passes”
  - Salesforce/IBM
  - Clear
- Fitbit – “Ready to Work” program
- Microsoft/United Healthcare – “ProtectWell” app
- Amazon – “Distance Assistant”



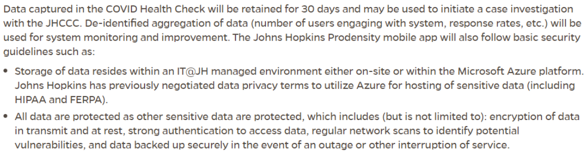
Lever – Post-COVID Workplace

- These systems “blur the lines between people’s workplace and personal lives … It erodes longstanding medical privacy protections for many different workers”
- “The invasion of privacy that workers face is alarming, especially considering that the effectiveness of these technologies in mitigating the spread of COVID-19 has not yet been established.”



Lever – Post-COVID Workplace

- Many companies are using third-party vendors to host the data and keep it separate.
- But many of these vendors have a business model centered on monetizing personal data.
- It’s all about a balance, the article concludes:
  - Employers have a legitimate interest in safeguarding workplaces and keeping employees healthy, but technologies are unproven.



Data captured in the COVID Health Check will be retained for 30 days and may be used to initiate a case investigation with the JHCCC. De-identified aggregation of data (number of users engaging with system, response rates, etc.) will be used for system monitoring and improvement. The Johns Hopkins Prodensity mobile app will also follow basic security guidelines such as:

- Storage of data resides within an IT@JH managed environment either on-site or within the Microsoft Azure platform. Johns Hopkins has previously negotiated data privacy terms to utilize Azure for hosting of sensitive data (including HIPAA and FERPA).
- All data are protected as other sensitive data are protected, which includes (but is not limited to): encryption of data in transmit and at rest, strong authentication to access data, regular network scans to identify potential vulnerabilities, and data backed up securely in the event of an outage or other interruption of service.

Solove – The Rise of the Digital Dossier

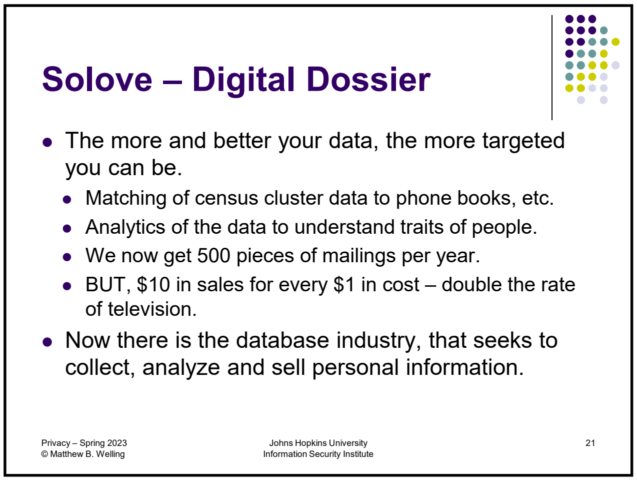
Is Your Personal Information Really Yours?

Solove – Digital Dossier

- Short history of public-sector databases:
  - Growth of the census.
  - Use of punch-cards and then computers allowed for processing of much more, and therefore collection of much more.
  - Led to privacy issues coming up in the 60s.
  - The Internet led to exponential growth – there are now* about 2,000 federal databases, and many state databases, all with important and sensitive personal data.

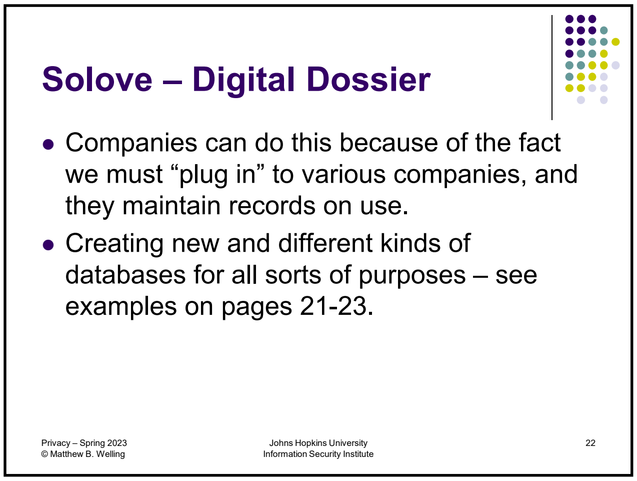
Solove – Digital Dossier

- Short history of Private-sector databases:
  - Personal marketing gave way to mass marketing, but only a small percentage purchased.
  - Led to "targeted marketing", i.e. finding out which people were most likely to consume a product and focus on them.
    - The GM example (targeted marketing to Ford owners).
    - Direct marketing, telemarketing.
  - The 2% rule (only 2% of those contacted by direct marketing actually respond)



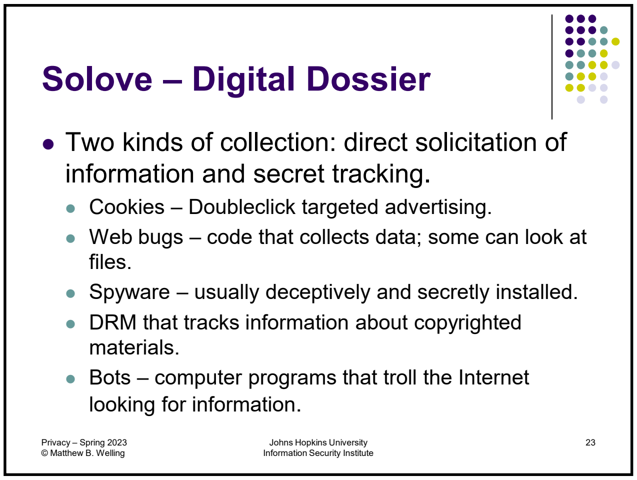
Solove – Digital Dossier

- The more and better your data, the more targeted you can be.
  - Matching of census cluster data to phone books, etc.
  - Analytics of the data to understand traits of people.
  - We now get 500 pieces of mailings per year.
  - BUT, $10 in sales for every $1 in cost – double the rate of television.
- Now there is the database industry, that seeks to collect, analyze and sell personal information.



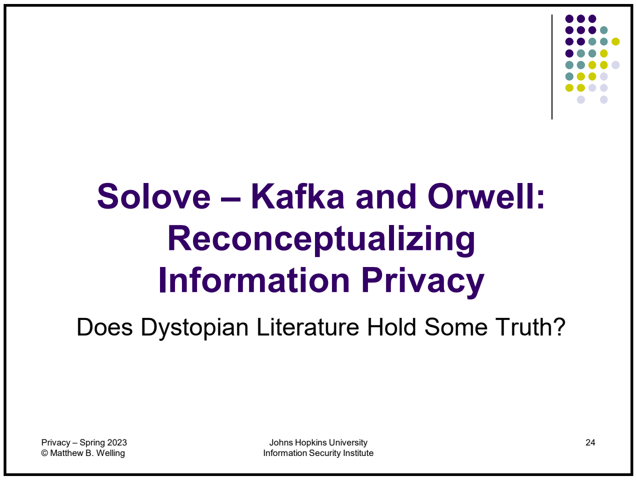
Solove – Digital Dossier

- Companies can do this because of the fact we must “plug in” to various companies, and they maintain records on use.
- Creating new and different kinds of databases for all sorts of purposes – see examples on pages 21-23.



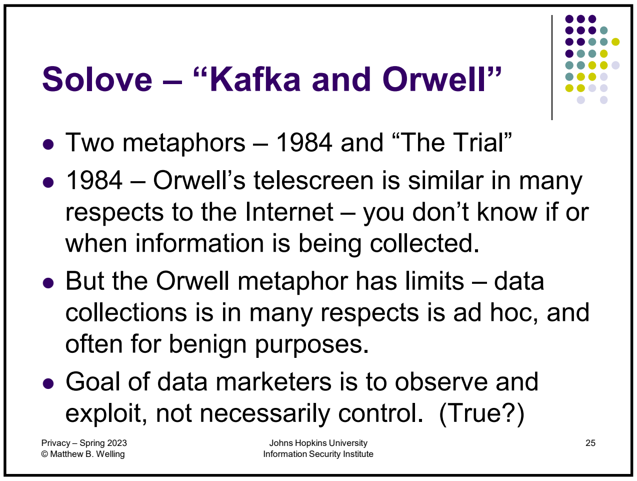
Solove – Digital Dossier

- Two kinds of collection: direct solicitation of information and secret tracking.
  - Cookies – Doubleclick targeted advertising.
  - Web bugs – code that collects data; some can look at files.
  - Spyware – usually deceptively and secretly installed.
  - DRM that tracks information about copyrighted materials.
  - Bots – computer programs that troll the Internet looking for information.



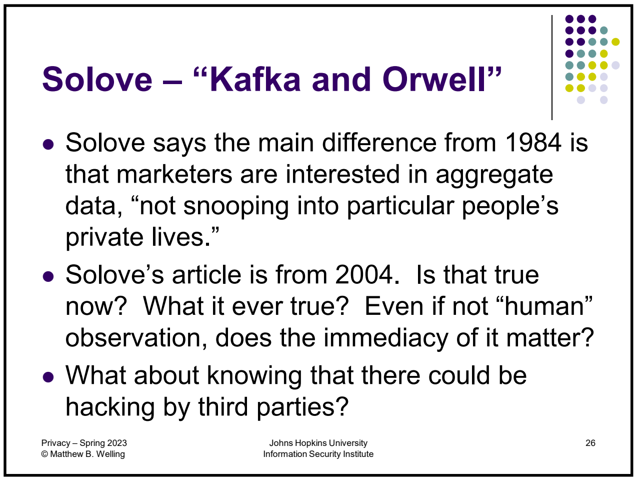
Solove – Kafka and Orwell: Reconceptualizing Information Privacy

Does Dystopian Literature Hold Some Truth?



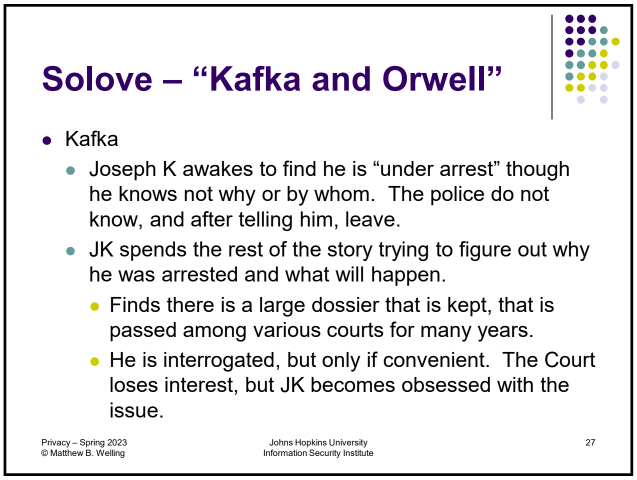
Solove – "Kafka and Orwell"

- Two metaphors – 1984 and "The Trial"
- 1984 – Orwell's telescreen is similar in many respects to the Internet – you don't know if or when information is being collected.
- But the Orwell metaphor has limits – data collections is in many respects is ad hoc, and often for benign purposes.
- Goal of data marketers is to observe and exploit, not necessarily control. (True?)



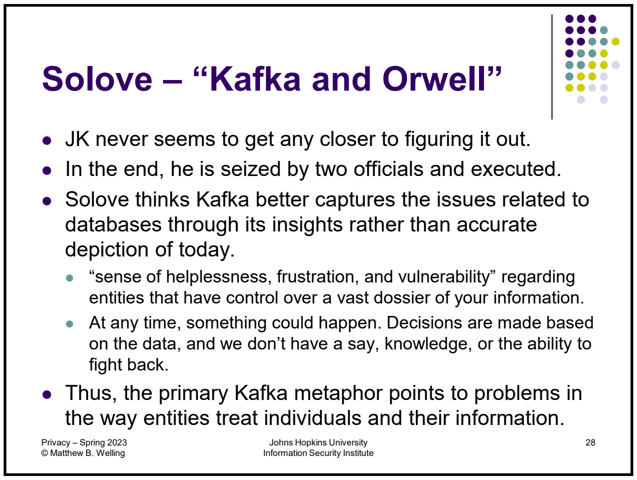
Solove – "Kafka and Orwell"

- Solove says the main difference from 1984 is that marketers are interested in aggregate data, "not snooping into particular people's private lives."
- Solove's article is from 2004. Is that true now? What it ever true? Even if not "human" observation, does the immediacy of it matter?
- What about knowing that there could be hacking by third parties?



Solove – "Kafka and Orwell"

- Kafka
  - Joseph K awakes to find he is "under arrest" though he knows not why or by whom. The police do not know, and after telling him, leave.
  - JK spends the rest of the story trying to figure out why he was arrested and what will happen.
    - Finds there is a large dossier that is kept, that is passed among various courts for many years.
    - He is interrogated, but only if convenient. The Court loses interest, but JK becomes obsessed with the issue.



Solove – "Kafka and Orwell"

- JK never seems to get any closer to figuring it out.
- In the end, he is seized by two officials and executed.
- Solove thinks Kafka better captures the issues related to databases through its insights rather than accurate depiction of today.
  - "sense of helplessness, frustration, and vulnerability" regarding entities that have control over a vast dossier of your information.
  - At any time, something could happen. Decisions are made based on the data, and we don't have a say, knowledge, or the ability to fight back.
- Thus, the primary Kafka metaphor points to problems in the way entities treat individuals and their information.

Solove – “Kafka and Orwell”

- Bureaucracies subject personal information to a process with little or no control or limit, which can limit “goals, wants, and needs.” Kafka shows how an imbalance in power, separate from any attempt to control, creates problems. He posits the same is true for databases.
- He recognizes (a little) that there may be an Orwellian component, i.e. targeted observation.
- Also, what about the compilation and cross-referencing of seemingly innocuous data? – the “Secrecy Paradigm”
- “Aggregation Effect” – a comprehensive collection is more than the sum of its parts.

Solove – “Kafka and Orwell”

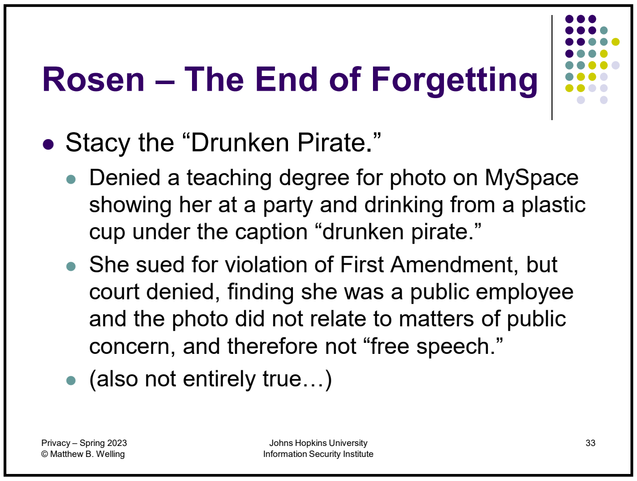
- What about inaccuracies? Solove provides examples…and then there’s this:
  - http://www.cbsnews.com/news/social-security-identity-fraud-scott-pelley-60-minutes/
- Solove then provides various other problems:
  - “Impoverished Judgments”
  - “Powerlessness and Lack of Participation”
  - “Problematic Information Gathering Techniques”
  - “Irresponsibility and Carelessness”
- In sum, per Solove, we’re heading to Kafka world.

Rosen – The End of Forgetting

Once it Goes on the Web, It’s There Forever

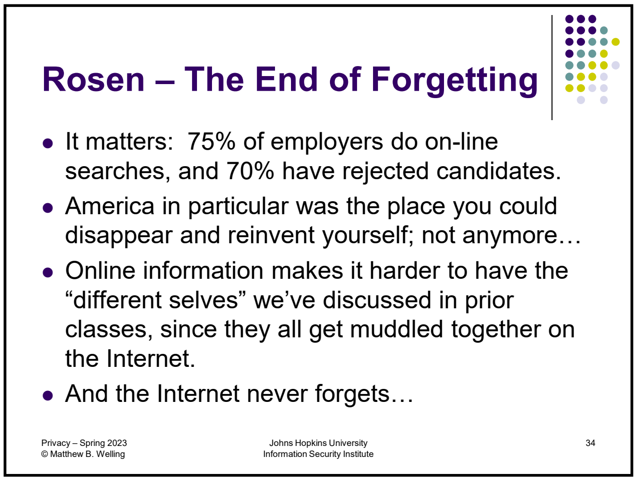
Rosen – The End of Forgetting

- Stacy the “Drunken Pirate.”



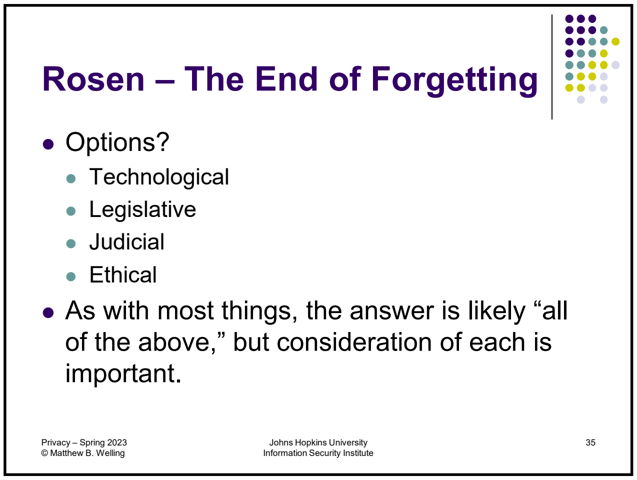
Rosen – The End of Forgetting

- Stacy the “Drunken Pirate.”
  - Denied a teaching degree for photo on MySpace showing her at a party and drinking from a plastic cup under the caption “drunken pirate.”
  - She sued for violation of First Amendment, but court denied, finding she was a public employee and the photo did not relate to matters of public concern, and therefore not “free speech.”
  - (also not entirely true…)



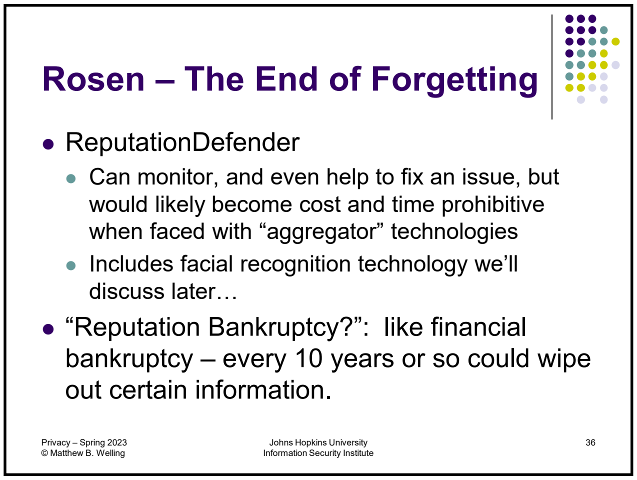
Rosen – The End of Forgetting

- It matters: 75% of employers do on-line searches, and 70% have rejected candidates.
- America in particular was the place you could disappear and reinvent yourself; not anymore…
- Online information makes it harder to have the “different selves” we’ve discussed in prior classes, since they all get muddled together on the Internet.
- And the Internet never forgets…



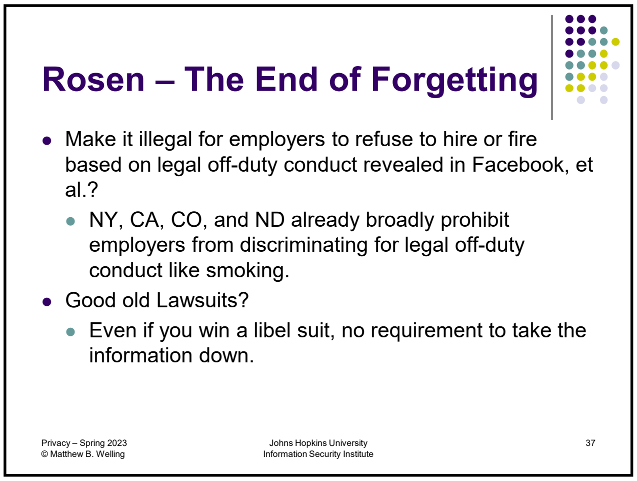
Rosen – The End of Forgetting

- Options?
  - Technological
  - Legislative
  - Judicial
  - Ethical
- As with most things, the answer is likely “all of the above,” but consideration of each is important.



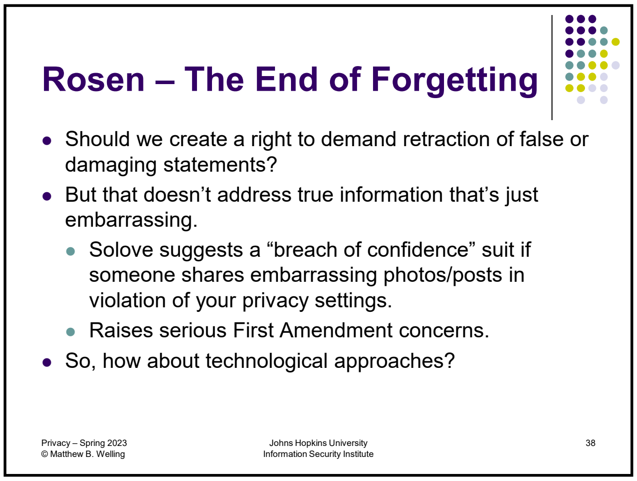
Rosen – The End of Forgetting

- ReputationDefender
  - Can monitor, and even help to fix an issue, but would likely become cost and time prohibitive when faced with “aggregator” technologies
  - Includes facial recognition technology we’ll discuss later…
- “Reputation Bankruptcy?”: like financial bankruptcy – every 10 years or so could wipe out certain information.



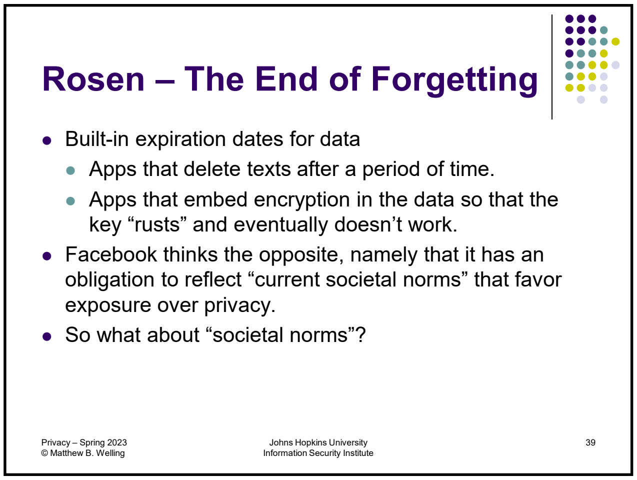
Rosen – The End of Forgetting

- Make it illegal for employers to refuse to hire or fire based on legal off-duty conduct revealed in Facebook, et al.?
  - NY, CA, CO, and ND already broadly prohibit employers from discriminating for legal off-duty conduct like smoking.
- Good old Lawsuits?
  - Even if you win a libel suit, no requirement to take the information down.



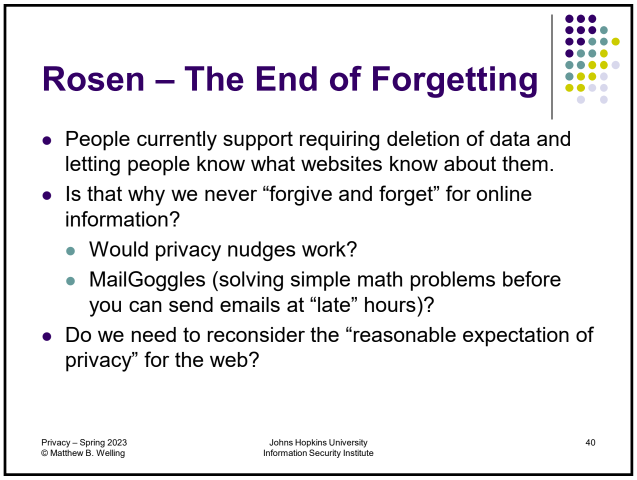
Rosen – The End of Forgetting

- Should we create a right to demand retraction of false or damaging statements?
- But that doesn't address true information that's just embarrassing.
  - Solove suggests a "breach of confidence" suit if someone shares embarrassing photos/posts in violation of your privacy settings.
  - Raises serious First Amendment concerns.
- So, how about technological approaches?



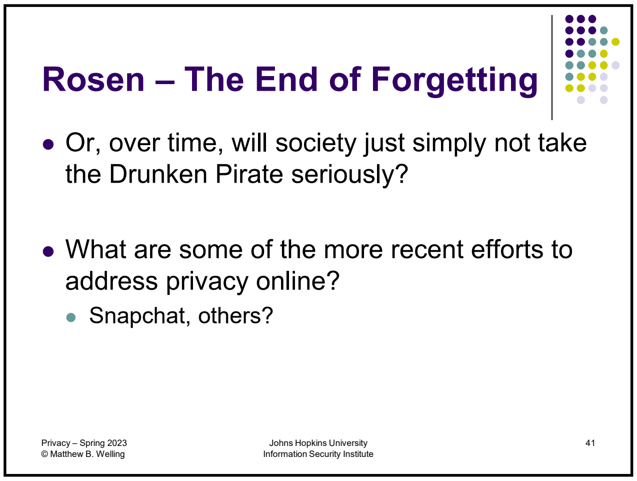
Rosen – The End of Forgetting

- Built-in expiration dates for data
  - Apps that delete texts after a period of time.
  - Apps that embed encryption in the data so that the key "rusts" and eventually doesn't work.
- Facebook thinks the opposite, namely that it has an obligation to reflect "current societal norms" that favor exposure over privacy.
- So what about "societal norms"?



Rosen – The End of Forgetting

- People currently support requiring deletion of data and letting people know what websites know about them.
- Is that why we never "forgive and forget" for online information?
  - Would privacy nudges work?
  - MailGoggles (solving simple math problems before you can send emails at "late" hours)?
- Do we need to reconsider the "reasonable expectation of privacy" for the web?



Rosen – The End of Forgetting

- Or, over time, will society just simply not take the Drunken Pirate seriously?
- What are some of the more recent efforts to address privacy online?
  - Snapchat, others?