Attendance update

• Please sign the attendance sheet before the break.
• The attendance sheet will be removed at the beginning of break during each class and you will no longer be able to sign it.
Announcements 3/1

• Briefing instructions today

• Next week is Spring Break – have fun!

• Please **show up for class March 15** – special guest speaker is **Andy Maltz from Oscars.org** on “Data and Entertainment”.

• **Class Wednesday March 13 / Student Presentations**

• **Topic Reports due March 15 for the first group** (group who will do their presentations on March 20)
Op-Ed Draft Grades

- **Only Op-Ed Final grades count.**

- You can turn your Draft Op-Ed grade into a Final Op-Ed grade by
  - Revising your Draft Op-Ed and turning in a Final Op-Ed on **March 29**
  - Letting Fran know by **March 28** that you want your Draft Op-Ed grade to be your Final Op-Ed grade

- No late work.
Grade Stuff

• For those who will turn in a Final Op-Ed on March 29
  – Revision will not be graded unless you also turn in Fran’s marked-up copy of the Draft Op-Ed
  – Final Op-Ed should be a revision based on Draft Op-Ed comments, not a new Op-Ed on a different topic
  – Final Op-Ed should be better than the Draft Op-Ed. Final Op-Ed grade will be recorded, even if it is lower than the Draft Op-Ed

• How to compute your Grade So Far (GSF):
  – GSF = 100 X \[
    [\text{Presentation Score} + \text{Op-Ed} + \text{Optimistic Participation}] / 40
  \]

• Optimistic Participation
  – Optimistic Participation means that you will not have any more unexcused absences for the rest of the semester and you participate in class discussion.
  – Optimistic Participation = 10 if you have missed at most 2 (unexcused) classes. If you have missed 2+k classes, your Optimistic Participation score is 10-k.
<table>
<thead>
<tr>
<th>Wednesday Section</th>
<th>Friday Lecture (first half)</th>
<th>Second half of class</th>
<th>Assts.</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 9: NO CLASS</td>
<td>January 11: INTRO – DATA AND SOCIETY</td>
<td>Fran presentation demo</td>
<td></td>
</tr>
<tr>
<td>January 16: NO CLASS</td>
<td>January 18: BIG DATA 1; Topic groups / Topic materials information</td>
<td>Student presentations</td>
<td></td>
</tr>
<tr>
<td>January 23: Student presentations</td>
<td>January 25: BIG DATA 2</td>
<td>Student presentations</td>
<td>Op-Ed instructions</td>
</tr>
<tr>
<td>January 30: NO CLASS</td>
<td>February 1: DATA AND SCIENCE</td>
<td>Student presentations</td>
<td></td>
</tr>
<tr>
<td>February 6: NO CLASS</td>
<td>February 8: DATA STEWARDSHIP AND PRESERVATION</td>
<td>Student presentations</td>
<td>Group Topics due</td>
</tr>
<tr>
<td>February 13: NO CLASS</td>
<td>February 15: INTERNET OF THINGS</td>
<td>Student presentations</td>
<td></td>
</tr>
<tr>
<td>February 20: Student presentations</td>
<td>February 22: DATA AND PRIVACY / FOUNDATIONS</td>
<td>Student presentations</td>
<td>Op-Ed Drafts due</td>
</tr>
<tr>
<td>February 27: NO CLASS</td>
<td>March 1: DATA AND PRIVACY / POLICY AND REGULATION</td>
<td>Student presentations</td>
<td>Briefing instructions Op-Ed Drafts returned</td>
</tr>
<tr>
<td>March 6: Spring Break</td>
<td>March 8: Spring Break</td>
<td>Student presentations</td>
<td></td>
</tr>
<tr>
<td>March 13: Student presentations</td>
<td>March 15: DATA AND ENTERTAINMENT [ANDY MALTZ]</td>
<td>Student presentations</td>
<td>Topic Reports 1 due</td>
</tr>
<tr>
<td>March 20: TOPICS PRESENTATIONS 1</td>
<td>March 22: DATA AND DATING</td>
<td>Student presentations</td>
<td></td>
</tr>
<tr>
<td>March 27: Student presentations</td>
<td>March 29: DIGITAL RIGHTS 1</td>
<td>Student presentations</td>
<td>Op-Ed Finals due</td>
</tr>
<tr>
<td>April 3: NO CLASS</td>
<td>April 5: DIGITAL RIGHTS 2</td>
<td>Student presentations</td>
<td>Briefings due</td>
</tr>
<tr>
<td>April 10: Student presentations</td>
<td>April 12: DATA AND ETHICS</td>
<td>Student presentations</td>
<td>Op-Ed Finals returned, Topic Reports 2,3 due</td>
</tr>
<tr>
<td>April 17: TOPIC PRESENTATIONS 2</td>
<td>April 19: CAREERS IN TECH [KATHY PHAM?]</td>
<td>Student presentations</td>
<td></td>
</tr>
<tr>
<td>April 24: Student presentations</td>
<td>April 26: TOPICS PRESENTATIONS 3</td>
<td>Student presentations</td>
<td></td>
</tr>
</tbody>
</table>
Lecture 8: Data Privacy 2

- Legal and policy frameworks for data privacy
  - Europe’s General Data Preservation Regulation
  - U.S.:
    - Privacy protections:
      - Federal: HIPAA, COPPA, FERPA, FCRA, etc.
      - States: Vermont data broker law, CA data privacy laws
    - Privacy of Research Data
    - Federal privacy legislation in-process
European Union (EU) Digital Agenda

- Overall aim is to deliver sustainable economic and social benefits to Europeans from information and communication technologies.
  
  - Europe perceives itself as lagging behind in terms of use and deployment if IT

- EU launched Europe 2020 strategy in March 2010. Digital Agenda for Europe one of the 7 flagship initiatives of the Europe 2020 Strategy. GDPR builds on work and legislation done in this area.
EU Data Challenges

• Fragmented digital markets
  – 27 countries in EU, much variation between content, services, and infrastructure across borders; unification difficult

• Lack of interoperability
  – “weaknesses in standard setting”, difficulty in coordination

• Rising cybercrime and low risk of trust in networks

• Lack of investment in networks

• Insufficient research and innovation efforts

• Lack of digital literacy and skills

• Missed opportunities in addressing societal challenges
EU Digital Agenda Action Areas 1

- **Single digital market**
  - Want to unify telecom, services, rules, and content
  - Rights and protection for consumers and businesses when doing business on-line

- **Interoperability and Standards**

- **Trust and security**
  - “Europeans will not embrace technology they do not trust – the digital age is neither ‘big brother’ nor ‘cyber wild west’.”
  (Digital Agenda for Europe, COM(2010) 245, 19.05.2010)
EU Digital Agenda Action Areas 2

• Fast and ultra fast internet access
  – Universal broadband coverage, open and neutral internet

• Research and Innovation
  – Leverage private investment and accelerate innovation
  – Increase digital literacy, skills and services

• ICT-enabled benefits for EU society
  – ICT-enabled energy, environment, health care, independent living, cultural diversity / arts, e-government, transportation.
Europe’s GDPR (General Data Protection Regulation)

• What is GDPR?
  – Regulation that protects EU citizens wrt the processing of personal data and the free movement of their data.
  – Passed by the EU Parliament in April 2016 and implementation commenced in May 2018.
  – Does not cover data personal data used in national security activities or law enforcement

• GDPR constitutes a single set of rules applies to all EU member states

• GDPR applies to any organization that collects data from EU residences or processes data from EU residents. *This includes multinational companies with EU customers.*
Key definitions

- **Data Subject**: Individuals whose data is being collected / processed / used. (Applicable to EU citizens)

- **Data Controller**: entity (individual or organization) that controls the procedures and purpose of data usage. (Controls the “how” and “why” of data usage).

- **Data Processor**: entity (individual or organization) that processes the data provided by a data controller.

- **Data Protection Officer**: Individual who is responsible for managing compliance with GDPR.

- **Supervisory Authority**: Independent (govt.) entity that can hear and investigate complaints, sanction administrative offenses, etc.

**Example:**

- Company X collects data on you when you visit their webpage
  - X = Data Controller
- Company X uses Google Analytics to track analytics data.
  - Google Analytics is Data Processor.
- Organizations can also be both (e.g. Google, Amazon)
GDPR and Data Privacy – Controller Responsibilities

- Controllers of personal data expected to put in place appropriate technical and organizational measures to implement data protection principles.

- Business processes that handle personal data must provide safeguards to protect data (for example, using pseudonymization or full anonymization where appropriate), and use the highest-possible privacy settings by default.
  - Data should not be made available publicly without explicit, informed consent, and cannot be used to identify a subject without additional information stored separately.

- No personal data may be processed unless it is done under a lawful basis, or unless the data controller or processor has received an unambiguous and individualized affirmation of consent from the data subject.
  - The data subject has the right to revoke this consent at any time.
Pseudonymization

• **Pseudonymization** is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

• GDPR definition of pseudonymization: “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.”

  – To pseudonymize a data set, the “additional information” must be “kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.”
GDPR and Data Privacy – Data Processor Responsibilities

• A processor of personal data must clearly disclose any data collection, declare the lawful basis and purpose for data processing, and state how long data is being retained and if it is being shared with any third parties or outside of [EU and Norway, Lichtenstein, and Iceland – free trade partners].

• Data subjects have the right to request a portable copy of the data collected by a processor in a common format, and the right to have their data erased under certain circumstances.

• Public authorities, and businesses whose core activities center around regular or systematic processing of personal data, are required to employ a data protection officer (DPO), who is responsible for managing compliance with the GDPR.

• Businesses must report any data breaches within 72 hours if they have an adverse effect on user privacy. In some cases, violators of the GDPR may be fined up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.
Many lawsuits
Real Penalties

- **Google fined 50M euros** for **not properly disclosing to users** how data is collected across its services (including browser, Google Maps, YouTube) to present personalized advertisements (NY Times, 1/19)

- **German social network operator fined 20,000 euros** for a **data security vulnerability** (not encrypting passwords, which were hacked [but then reported expeditiously]). Smaller fine because company complying with Supervisory Authority recommendations.

- **Reprimands to Swedish companies** that have **not appointed a Data Protection Officer**.

- **5,289.00 euro fine imposed on Austrian LLC running a sports betting café for video surveillance** (parking lot, entrance). Controller was fined for insufficient processing logs, inadequate signage, insufficient justification for extended storage period.
GDPR – A Work in Progress

• Many kinds of impact:
  – Multinational companies changing privacy infrastructure to comply and other companies following suit for national privacy laws to come
    • Some companies choosing not to sell to Europeans
  – U.S. and other countries getting more serious about privacy laws
  – Disproportionate effort for smaller businesses (costs of compliance, DPO, etc.)
  – More responsibility on the “C-suite” for compliance
U.S. Data Privacy Landscape

• No single, comprehensive federal U.S. law regulating the collection and use of personal data.

• US has a patchwork system of federal and state laws, and regulations that can sometimes overlap, dovetail and contradict one another. Also government agency guidelines that are considered “best practices”.

• The combination of an increase in interstate and cross-border data flow, together with the increased enactment of data protection-related statutes heightens the risk of privacy violations and creates a significant challenge for a data controller to negotiate the onerous and often inconsistent requirements for each state, when operating at a national level.
U.S. Data Privacy Laws -- Timeline

The following are some of the laws, regulations and directives related to the protection of information systems and private information in the U.S. up to 2002 [Wikipedia]:

- 1970 U.S. Fair Credit Reporting Act
- 1970 U.S. Racketeer Influenced and Corrupt Organization (RICO) Act
- 1974 U.S. Privacy Act
- 1974 Family Educational Rights and Privacy Act (FERPA)
- 1980 Organization for Economic Cooperation and Development (OECD) Guidelines
- 1984 U.S. Medical Computer Crime Act
- 1986 U.S. Electronic Communications Privacy Act (ECPA)
- 1988 U.S. Video Privacy Protection Act
- 1990 United Kingdom Computer Misuse Act
- 1992 OECD Guidelines to Serve as a Total Security Framework
- 1994 Communications Assistance for Law Enforcement Act
- 1996 U.S. Economic and Protection of Proprietary Information Act
- 1996 Health Insurance Portability and Accountability Act (HIPAA) (requirement added in December 2000)
- 1998 U.S. Digital Millennium Copyright Act (DMCA)
- 1999 U.S. Uniform Computer Information Transactions Act (UCITA)
- 2000 U.S. Congress Electronic Signatures in Global National Commerce Act ("ESIGN")
- 2001 U.S. Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act
- 2002 Homeland Security Act (HSA)
U.S. Data Privacy Laws -- HIPAA

Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.) Regulates medical information. Can apply broadly to health care providers, data processors, pharmacies and other entities that come into contact with medical information.


• HIPAA enacted by Congress in 1996.

• Basic idea of HIPAA is that an individual who is a subject of individually identifiable health information should have:
  - Established procedures for the exercise of individual health information privacy rights.
  - The use and disclosure of individual health information should be authorized or required.

• Challenges:
  - Consent is problematic under HIPAA, because the medical providers simply make care contingent upon agreeing to the privacy standards in practice.
  - There must be a mechanism to authenticate the patient who demands access to his/her HIPAA data. As a result, medical facilities have begun to ask for Social Security Numbers from patients, thus arguably decreasing privacy by simplifying the act of correlating health records with other records.
**COPPA**

- **Children's Online Privacy Protection Act (COPPA)** passed in 1998 and effective in 2000 is a U.S. federal law that applies to the online collection of personal information by U.S. children under 13.

- Websites must protect children's privacy and safety online including restrictions on the marketing of those under 13.
  - Applies to commercial websites and online services operated for either directed towards children under 13 or have knowledge that children under 13 are providing information online.
  - Website operators must have privacy policies and seek verifiable consent from a parent or guardian.
  - FTC enforces COPPA.

- **To comply**, commercial websites must:
  - Provide a clear privacy policy.
  - Provide reasonable means for a parent to review personal information collected from their child and be able to refuse to permit its use and maintenance.
  - Retain personal information collected on-line only as long as necessary to fulfill its purpose.
  - Not condition children’s participation by having the child provide more information than is reasonably necessary to participate.
  - Ensure that any third parties to whom children’s information is disclosed must have reasonable procedures in place to protect information.
FCRA

- The 1970 **Fair Credit Reporting Act (FCRA)** is a federal law that promotes accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies.
  - Intended to protect consumers from the willful and/or negligent inclusion of inaccurate information in their credit reports.
  - Updated in 2003 as FACTA (Fair and Accurate Credit Transaction Act). FACTA allows affiliate sharing of credit reports, “prescreening” of credit reports (unsolicited offers of credit to certain customers) and limited preemption of stronger state credit laws.

- FCRA regulates the collection, dissemination, and use of consumer information, including consumer credit information.
  - Enforced by the US Federal Trade Commission, the Consumer Financial Protection Bureau and private litigants.

- Credit reports used for background checks, insurance, employment, credit checks, etc.
  - 2015 report showed that 23% of consumers identified inaccurate information in their credit reports. (You can get one free credit report from annualcreditreport.com per year to identify inaccurate information).

- You can increase the privacy of your information beyond FCRA (and related regulations) by
  - Opting out of prescreening
  - Opting out of marketing offers from affiliate sharing
  - Opting out of affiliate information sharing
  - Requesting that Credit Reporting Agencies withhold the last five SSN digits when supplying credit reports
  - [See https://www.epic.org/privacy/fcra/ for how]
FERPA

- The **Family Educational Rights and Privacy Act** of 1974 (FERPA or the **Buckley Amendment**) is a United States federal law that governs the access of educational information and records to public entities such as potential employers, publicly funded educational institutions, and foreign governments.
  - FERPA gives parents access to their child's education records, an opportunity to seek to have the records amended, and some control over the disclosure of information from the records.
  - With several exceptions, schools must have a student's consent prior to the disclosure of education records after that student is 18 years old.

- The law applies only to educational agencies and institutions that receive funding under a program administered by the U.S. Department of Education.

- **FERPA protects “educational records”:**
  - Grades
  - Class lists
  - Student course schedules
  - Disciplinary records
  - Student financial records
  - Payroll records for employees who are employed as a result of their status as students (RAs, TAs, Resident Assts, etc.)

- **FERPA doesn’t protect**
  - “Sole possession” records made by faculty and staff for their own use and not shared
  - Personal observations
  - University law enforcement records
  - Medical and mental health records used to treat students
  - Alumni records
  - Peer-graded papers and exams prior to the grade being recorded
Data Privacy and Research

- Privacy applies to both research results and research subjects (participants in clinical trials, social science research, collections of human specimens, genetic information, etc.)
  - Privately funded research used for private organization (e.g. a company); often precludes public reporting of results
  - Privacy of research subjects managed in academic institutions by IRB (Institutional Research Board)
  - Federal agencies expect research to be publicly disseminated unless it would violate privacy rights (e.g. HIPAA)

Informed Consent: permission granted in the knowledge of the possible consequences

https://www.nytimes.com/2010/04/22/us/22dna.html, more about this case in subsequent lectures
State Privacy Laws

• There are many laws at the state level that regulate the collection and use of personal data, and the number grows each year.
  – Some federal privacy laws pre-empt state privacy laws on the same topic. Companies may find themselves in the position of complying with both.

• Most states have enacted some form of privacy legislation, however California leads the way in the privacy arena, having enacted multiple privacy laws, some of which have far-reaching effects at a national level. Unlike many federal privacy laws in the US, California's privacy laws resemble the European approach to privacy protection.
  – California is one of only a handful of states to create an Office of Privacy Protection (www.privacy.ca.gov).

• Resource for privacy laws by state:
  https://www.epic.org/privacy/consumer/states.html

Fran Berman, Data and Society, CSCI 4370/6370
California Privacy Laws

Right to privacy guaranteed in State Constitution:

- **ARTICLE I DECLARATION OF RIGHTS [SECTION 1 - SEC. 32]** *(Article 1 adopted 1879.)*
- **SECTION 1.** All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. *(Sec. 1 added Nov. 5, 1974, by Proposition 7. Resolution Chapter 90, 1974.)*

Major privacy protection laws at the California State and federal level.

- **California Law - General Privacy Laws**
  - Automated License Plate Recognition Systems, Automobile black boxes
  - Financial code, bank account numbers
  - Computer misuse and abuse – criminal sanctions, Electronic communications privacy, connected televisions
  - Consumer credit reporting
- **California Law - Health Information Privacy**
- **California Law - Identity Theft**
- **California Law - Online Privacy**
- **California Law - Unsolicited Commercial Communications**
California Data Privacy Laws

• **Shine the Light law** (Cal. Civil Code. §§1798.83-1798.84) *Requires companies to disclose details of the third parties with whom they have shared their personal information.*

• **Data security law** (Cal. Civil Code §1798.81.5) *Requires businesses to implement and maintain reasonable security procedures to protect personal information from unauthorized access, destruction, use, modification, or disclosure.*

• **Security Breach Notification law** (California Civil Code §1798.82) *Requires any person or business that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system to all California residents whose unencrypted personal information was acquired by an unauthorized person.*
California Consumer Privacy Act of 2018

- Act gives “consumers” (defined as natural persons who are California residents) four basic rights in relation to their personal information:
  1. The right to know, through a general privacy policy and with more specifics available upon request, what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold;
  2. The right to “opt out” of allowing a business to sell their personal information to third parties (or, for consumers who are under 16 years old, the right not to have their personal information sold absent their, or their parent’s, opt-in);
  3. The right to have a business delete their personal information, with some exceptions; and
  4. The right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.

- The Act’s provisions are designed to put these rights into practice.
- Goes into effect 1/1/2020.
Some differences between the California Act and GDPR (other than the obvious …)

• **GDPR is an omnibus law, while the Act is not.**
  
  – GDPR regulates what disclosures companies must make to data subjects, and also covers procedures for data breach notification to individuals and regulators, data security implementation, cross-border data transfers and more.
  
  – California Act is more limited, as it primarily is concerned with consumer privacy rights and disclosures made to consumers.

• **Both GDPR and the Act give consumers certain rights as to their personal data, but those rights differ somewhat.**
  
  – While both the GDPR and the Act grant users the right to know what personal information a company has about them, Articles 15 and 20 of the GDPR impose additional requirements as to which data must be shared with the user, and the manner in which the disclosure must be made. Further, the

• **GDPR offers a some rights to data subjects that California Act does not**
  
  – These include the right to be forgotten, the right to rectification, and the right to not be subject to a decision based solely on automated processing.
Vermont Data Broker Law (H.764)
(from https://www.lexology.com/library/detail.aspx?g=5398e04c-f672-428e-b8f6-707538072acf)

- **Data broker** = a business that "knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship."

- Goal of the law is to regulate businesses that collect, aggregate, and sell data about consumers with whom the business **does not** have a relationship.
  - Businesses that collect, share, or sell their own consumers' data **are not** affected by this law, so long as they have a direct business relationship with those consumers.
  - Applies to Vermont residents (consumers) and businesses from anywhere

- Law is the first of its kind in the United States.

- Penalties:
  - Violations of the law are considered **unfair and deceptive acts** under Vermont law
  - Vermont Attorney General has the authority to conduct civil investigations, bring civil actions, and take other enforcement actions allowed by the law against the data broker.

- The law became effective **January 1, 2019.**
Obligations imposed on data brokers

- Data brokers forbidden from acquiring brokered personally identifiable information by fraudulent means, as well as using this information to stalk, discriminate, commit fraud, etc.

- Data brokers must disclose their practices to consumers by providing them with contact information, giving them the opportunity to opt out of data collection, and disclosing recent security breaches.

- Data brokers must register annually with the Vermont Secretary of State.

- Data brokers have heightened obligations to protect personal information, including maintaining a comprehensive security program to protect this information.

- Data brokers must make annual disclosures to the Vermont State Attorney General.
What kind of infrastructure is needed to protect your privacy?

• **Where** should various kinds of data live?
• **Who** should have access, control, usage rights, and when?
• What are reasonable expectations for metadata, interoperability, openness, security, **stewardship, preservation**?
• What are appropriate **retention policies** for various kinds of IoT data
• **Who should pay** for infrastructure?
• How do we do **open science** on private data?
• How do we do **reproducible research** on private data?
How much does it matter if your data is private?

• When should your data be private?
• Where should your data be private?
• Under what circumstances should you be compelled to give up your privacy?
Lecture 8 References (not already on slides) 1

- GDPR Impact, [https://digiday.com/media/impact-gdpr-5-charts/](https://digiday.com/media/impact-gdpr-5-charts/)
• COPPA, FCRA, FERPA, Wikipedia
• Fair Credit Reporting Act, EPIC, https://www.epic.org/privacy/fcra/
• “You need to understand your educational privacy rights”, Forbes, https://www.forbes.com/sites/willarddix/2018/05/16/you-need-to-understand-your-educational-privacy-rights/#7807ed576b93
Briefing Instructions
What is a briefing paper?
(adapted from WikiHow
https://www.wikihow.com/Write-a-Briefing-Paper)

• A briefing paper outlines a particular issue and its background, usually for a stakeholder. Briefing papers often propose solutions / improvements.
  – Stakeholders are decision-makers who often have to make hard choices about topics that they do not have time to research in-depth.

• A briefing paper fills in key details he or she needs to know. It often proposes solutions and recommends improvements as well that tell the stakeholder how they can help.

• A briefing paper is brief, concise, well-organized, covers the most important and relevant facts and issues, and proposes a helpful action.

Briefing Paper structure:

• Who is your stakeholder? Describe who the briefing paper is being written for. (One sentence)

• Subject – The responsible use of data in <topic of your own choosing>

• Background
  – Concise summary of past and/or current events that provides a context for the topic or issue, including any policies or past practices

• Analysis
  – What are significant aspects of the topic or issue
  – What is the impact of your chosen topic on society?
  – What can the stakeholder do to address this topic?

• Summary paragraph
  – Key takeaways from your paper

• References (not counted in page count)
“Informative” Briefing Assignment

• **What**: Write a briefing (2 pages undergrads, 3 pages grads, 11 pt. font, 1.5 line spacing) paper on “The responsible use of data in <topic of your own choosing>”. Briefings are worth at most 10 points.

• **When**: Briefings are due at the beginning of class on April 5; please turn in a hardcopy to Fran. No late work.

• **Who writes this**: You, by yourself

• **Good info on this at** [https://www.wikihow.com/Write-a-Briefing-Paper](https://www.wikihow.com/Write-a-Briefing-Paper)

---

**How you’ll be graded:**

• **Content**: 5 points
  – Is the data story cohesive?
  – Are the issues and analysis relevant?
  – Is the information pertinent to the issue?
  – Is the solution actionable?

• **Writing**: 5 points
  – Is the writing compelling, concise and informative
  – Does the piece read well? Is it informative?
  – Is the spelling and grammar correct? Is the piece well-referenced?
Presentations to be assigned
March 15


• “Music’s Moneyball moment: Why data is the new talent scout,” Financial Times, https://www.ft.com/content/474ae18a-7f1b-11e8-bc55-50daf11b720d [Chang X.]


• “Has Artificial Intelligence brought us the next great art movement? Here are 9 pioneering artists who are exploring AI’s creative potential,” Artnet News, https://news.artnet.com-market/9-artists-artificial-intelligence-1384207 [Korryn R.]
March 22

- “Can Alexa and Facebook predict the end of your relationship?”, Vox, [link](https://www.vox.com/the-goods/2019/1/2/18159111/amazon-facebook-big-data-breakup-prediction) [Rahul D.]


- “Shady data brokers are selling online dating profiles by the millions,” Motherboard, [link](https://motherboard.vice.com/en_us/article/59vbp5/shady-data-brokers-are-selling-online-dating-profiles-by-the-millions) [Rufeng M.]

- “OKCupid study reveals the perils of big data science.”, Wired, [link](https://www.wired.com/2016/05/okcupid-study-reveals-perils-big-data-science/) [Yawen S.]
Break
Presentation Articles for March 13

• “Find out if your password has been pwned – without sending it to a server,” Ars Technica, https://arstechnica.com/information-technology/2018/02/new-tool-safely-checks-your-passwords-against-a-half-billion-pwned-passwords/ [Andrew L.]


Presentation Articles for Today


- “How Microsoft has (so far) avoided any scrutiny over privacy issues”, Fast Company, [https://www.fastcompany.com/90290137/how-microsoft-has-avoided-tough-scrutiny-over-privacy-issues](https://www.fastcompany.com/90290137/how-microsoft-has-avoided-tough-scrutiny-over-privacy-issues)