Your Data and Democracy:

A Workshop on Political Action for Data Privacy

IS 272: Human Computer Interaction
Professor Lievrouw

Jessica Craig
Malak Hmimy
Alexandra Solodkaya
Shota Vashakmadze

Introduction

Data privacy is a complicated issue with many components. There are numerous types of data created by and about individuals, and there are limits to the control that any one person exercises over their creation and release. Some data, like medical records, has stringent legal protection, while other types of data, like consumer data and data generated on social media platforms, have no such protections. Unprotected data is not only accessible to any and all who care to find it, but it can also be used in novel ways for profit and for control.

Many of us are now aware of the types of ways our data can be used for profit. Data aggregators can trace individual digital footprints and package them into tidy consumer profiles to advertisers and marketers for a fee. Sites like Facebook and Twitter deliver targeted advertising to users based on user profiles, preferences and likes. Google collects user search history (Google Search), location information (Google Maps) and scans all communications and files created on their suite of tools (GMAIL, Google Docs and Sheets etc.) in order to deliver targeted advertising. The ability of private companies to profit from data collection in this way may seem like a benign threat, or only slightly invasive. To some it may seem like a small price to pay for the convenience of the services offered in return. But when you begin to realize the extent of the data captured[1] and the ways that this data can be weaponized by governments, financial institutions, law enforcement, etc.[2] the results are chilling.

A recent example of weaponized data is the purchase of location information by US Customs and Border Patrol and the Department of Homeland Security to track and apprehend people who may be in the US illegally.[3] Gilad Edelman explains that because CBP and DHS are purchasing this information from third party aggregators this may allow them to circumvent the Fourth Amendment, which protects Americans from "unlawful search and seizure."[4] An

---

[1] Dylan Curran, "Are You Ready? This Is All the Data Facebook and Google Have on You," *The Guardian*, March 30, 2018, sec. Opinion, https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy.

[2] Bruce Schneier, "We're Banning Facial Recognition. We're Missing the Point.," *The New York Times*, January 20, 2020, sec. Opinion, https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html.

[3] Gilad Edelman, "Can the Government Buy Its Way Around the Fourth Amendment?," *Wired*, February 11, 2020, https://www.wired.com/story/can-government-buy-way-around-fourth-amendment/.

[4] Edelman, 2020.

article by the New York Times Editorial Board on the same issue insists that because location information is being purchased on-mass, instead of on a case-by-case basis, this practice circumvents due-process and results in what Justice Roberts has called 'near perfect surveillance' of US citizens.[5] Facial recognition technology, largely built from publicly available photographs on sites like Facebook and Flickr, is another example of weaponized data capture. Using tools like Clearview AI, police departments and other governmental and private agencies, can now easily identify images of persons of interest and connect them to any and all online profiles.[6]

Faced with the level and scope of data weaponization it is naive to think that efforts to protect privacy on an individual level, through personal device, application and browser settings, could be effective enough to insure our protection from overreaches by government and law enforcement. It is imperative that concerned citizens begin to act politically calling on policy and law makers to build these protections. Both Edelman and Charlie Warzel[7] writing for the New York Times Privacy Project Series calls on Congress to take up the overarching issue of data privacy and protection. Making the weaponization of data that has already been collected or could be collected in the future illegal is the only way to ensure our protection.

Taking the need to act politically as the basic premise of our workshop, we will focus on educating participants about various forms of data collection and how it can be weaponized, and then empowering them to connect with lawmakers and politicians to make their voices and opinions about the need for overarching data privacy protection heard. It is only through the use of our democratic systems to enact legally binding and enforced protections that any lasting change can be created.

The workshop will consist of four sections. Section One will introduce the topic of data collection and lead participants through an individual activity that familiarizes them with

---

[5] The Editorial Board, "The Government Uses 'Near Perfect Surveillance' Data on Americans," *The New York Times*, February 7, 2020, sec. Opinion, https://www.nytimes.com/2020/02/07/opinion/dhs-cell-phone-tracking.html.
[6] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, January 18, 2020, sec. Technology, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[7] Charlie Warzel, "We Need a Law to Save Us From Dystopia," *The New York Times*, January 21, 2020, sec. Opinion, https://www.nytimes.com/2020/01/21/opinion/facial-recognition-privacy-law.html.

the common ways that data about individuals is collected. Section Two will be a lecture that introduces the idea of data weaponization and how governments and law enforcement can use unprotected data to target large swaths of the population. Section One and Two are explicitly about data. Section Three will ask participants to work together in groups to dive into how the data collection discussed in Sections One and Two impacts their own lives. In this section participants will learn how to clearly articulate at least one concern about data privacy. In Section Four participants will learn how to connect to the policy makers and public officials that represent them. These officials will be selected based on their ability to respond to concerns about data privacy and protection. Section Three and Four are geared toward framing data collection as a political issue and encouraging participants to use the democratic process to make their voices heard.

Workshop Audience

Given the time, place, and the nature of this workshop, we determined that it would be best if the target audience was composed of members from the UCLA community—more specifically UCLA undergraduate and graduate students. These groups make up the largest statistical percentage of the UCLA community and would theoretically be the largest population present at the workshop presentation. Narrowing the audience down to UCLA students makes it possible to make preliminary assumptions about the technological competency, and familiarity with mobile applications and websites of the audience. It also encompasses the eighteen to twenty-four, twenty-five to thirty-four, and thirty five to forty-four age groups, which include some of the age groups with the highest social and professional usage of technological platforms that typically collect large quantities of user data.

Further, narrowing the target population allows the workshop content to be more sensitive to demographic information shared by a large majority of the selected audience, such as socioeconomic status, and more; it also allows the content of the workshop to be more sensitive to the goals, motivations, and challenges of the target audience.

Three personas were created in order to represent the typical audience. Some considerations

that were taken into account when crafting these personas were the typical student experiences, diversity, and career trends of students enrolled at UCLA. Collectively, the personas represent groupings of UCLA students and their likely individual interactions and level of concern in regard to personal data collection.

The first persona, Mona, represents the many newly admitted first-year undergraduate, traditional students, as well as any student who may have limited computer literacy and likely an accompanying general lack of cognizance about data privacy concerns. The second persona, Amy, roughly represents the graduate and professional school students enrolled at UCLA, as well as students who may have preexisting sentiments and/or experiences regarding data privacy concerns as well as involvements in advocacy and/or activism. The third persona, Jamie, represents the non-traditional students at UCLA and the many students who are studying highly technical or scientific academic disciplines and may have intermediate levels of experience surrounding data privacy concerns. Jamie also represents the large percentage of students at UCLA who intend to work in the large technology sector that dominates California's economy and is the primary perpetuator of data privacy concerns.

See Appendix A for User Personas

Topic Map and Workshop Outline

The themes of our workshop, in their specific subject matter, as well as our broader premise of political intervention, are linked together by the deep and complex technological infrastructures that determine how data is generated and managed. The technologies we are dealing with are greatly interdependent, and their effects on society are not easily understood. As such, we have to engage our topics on their own terms while recognizing the limits of what they can each articulate. This means a broad view, but one that is not necessarily comprehensive, and an approachable way of framing personal relationships to data as political. We will outline three categories in parallel: consumer data, location data, and health data, as three sites that connect immediate personal actions to economic and

political structures beyond the control of individuals. Tracing these topics, we will translate them into models of political engagement that aim to account for this expansive scale.

Consumer Data: This category will encompass the management of data about the consumption habits of individuals, as they relate to advertising and the definition of a “data double” that has tangible effects on users’ lives. The scope of data in this topic is broad, ranging from credit scores to brand affinities, and compiled from many unrelated sources. What the workshop will hope to make clear is the way in which the proliferation of this data is related to its limited regulation, and how this regulation should be a priority over personal practices intended to limit users’ exposure.

Location Data: This topic deals with production and commerce in geospatial tracking data, whether used for integration into consumer databases or more invasive surveillance. This data can be produced directly, by GPS or cell tower triangulation, or it can be inferred from other information, relying on a combination of specific technologies and access to specific data sets to commodify private activity. The legislative approach to this topic will confront issues of state power and surveillance, especially through coordination with commercial data providers.

Health Data: The category will address the medical information generated by health tracking technologies and the clinical medical records of individuals. Of great significance here are the privacy issues surrounding the monetization of medical data, in which our bodies are transformed into a source of marketable commodities, often without the necessary consent. The workshop’s strategy of asserting political and legislative control over this data ties directly into its reliance on weak regulations to maintain economic value, problematized most directly in its role in a for-profit healthcare industry.

While these are our starting points, they should not preclude discussion of other categories that reveal analogous relationships between individuals and the production of data, and we expect conversations to expand beyond our particular starting points. The learning outcomes of our workshop rely on this strategy, raising questions about their overlaps, similarities, and differences, and aiming to take what is familiar about these types of data

and further consider the social consequences their tacit acceptance entails. Likewise, our activities are designed to bridge the personal and the political, using the scale of users' involvement with these data to suggest a similar agency in political organization. We hope that the takeaways can also reach beyond the specific questions of personal data and provoke critical thought about technology and political agency in other contexts.

Workshop Outline:

Section 1: Introducing the problem (25 minutes)
Learning Objective 1: Participants will gain an understanding of what data is being collected about them.

Intro Lecture (5 minutes)

Individual Activity (Activity 1): (20 minutes)
pass out Handout 1

Consumer Data i.e.: Google Ad Data; Facebook ad tracking
Location Data i.e.: Google Maps:
Health Data i.e.: Health(iOS); Genetic testing (23 and Me, Ancestry)

Section 2: How data sources intersect (20 minutes)
Learning Objective 2: Participants will gain an understanding of the potential and unforeseen implications of data collection.

Lecture: Examples of Data weaponization

Consumer Data:

Example A: South Dakota DMV / Student Loan data[8]
Example B: Facebook ethnic affinity categories and fair housing[9]

Location Data:

Example A: ICE purchasing location data from cell phone providers[10]

Health Data:

Example A: Health providers and health insurance companies as targets for data breach[11]

---

[8] Erika Leigh, "State Law Sparks Student Debt Controversy," last modified September 20, 2017, https://www.dakotanewsnow.com/content/news/State-law-sparks-student-debt-controversy-446255773.html.
[9] Julia Angwin and Terry Parris Jr., "Facebook Lets Advertisers Exclude Users by Race, last modified, October 28, 2016, "https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race.
[10] Rani Molla, "Law Enforcement is Now Buying Cell Phone Location Data from Marketers" last modified February 7, 2020, https://www.vox.com/recode/2020/2/7/21127911/ice-border-cellphone-data-tracking-department-homeland-security-immigration.
[11] "Attorney General Ferguson's Investigation into Premera Data Breach Results in Premera Paying $10 Million Over Failure to Protect Sensitive Patient Data" *Office of the Attorney General*, July 11, 2019,

Section 3: How you're data is tracked impacts you! (30 minutes)
Learning Objective 3: Participants will be able to articulate one data collection issue that concerns them.

Group Activity (Activity 2): Split into 3 groups, each one addresses either a) consumer data b) location tracking or c) health data.
pass out Handout 2

Section 4: Learn how to Act Politically! (35 minutes)
Learning Objective 4: Participants will be able to strategize ways to connect to and put pressure on public officials and institutions regarding the data collection issue they are concerned with.

Introduce tools/resources: (5 minutes)
pass out Handout 3

Group activity (Activity 3): (20 minutes)
Maintain 3 previous groups and investigate who you can contact and how you would approach them.

Debrief (10 minutes)
Recap findings of the activity, discuss broader context (immigration status, differences between local/state/federal, following up)

Wrap up: (10 minutes)
Summarize activities and learning outcomes

Learning Objectives:

Our learning objectives for the workshop are divided between our two identified topic areas, educating participants about data collection and encouraging political action for data privacy protection. The objectives are tied to each of the four sections of the workshop, and are scaffolded to insure effectiveness. Because each learning objective builds upon the previous one, and there are two clear topic areas, the workshop could easily be adapted to be delivered in two parts.

Our learning objectives related to data collection are:

- Objective 1 (Section One): Participants will gain an understanding of what data is

https://www.atg.wa.gov/news/news-releases/attorney-general-ferguson-s-investigation-premera-data-breach-results-premera.

being collected about them.

- Objective 2 (Section Two) - Participants will gain an understanding of the potential and unforeseen implications of data collection.

Learning Objectives 1 and 2 fall within the cognitive domain of Bloom's Taxonomy of Educational Objectives,[12] specifically within the knowledge category. As participants are introduced to the topic of data collection, and the unforseen consequences of this collection they will gain knowledge about the topic. After the first two sections of the workshop participants should be able to define data collection, recall examples of different forms of data collection and recall some of the unforeseen consequences of this collection.

Our learning objectives related to political action are:

- Objective 3 (Section Three) - Participants will be able to articulate one data collection issue that concerns them.

- Objective 4 (Section Four) - Participants will be able to strategize ways to connect to and put pressure on public officials and institutions regarding the data collection issue they are concerned with.

Learning Objectives 3 and 4 also fall within the cognitive domain of Bloom's Taxonomy but address comprehension and application. Learning Objective 3 displays comprehension in the form of synthesis and explanation. Participants must learn to explain their issue, why they care and why others should care. Synthesis and explanation are very important because Section Four will ask participants to communicate their articulated issue to a policy maker, representative or other person in a position of power able to help them in their fight for data privacy protection. Learning Objective 4 asks participants to apply the knowledge and comprehension that they've gained in the previous sections of the workshop by using it to connect to policy makers. We will be able to judge successful attainment of each learning objective by the ability of participants to move from one workshop activity to the next. If participants have built the necessary skill in the previous section, they should be able to move seamlessly through the next section.

---

[12] Norman Edward Gronlund, *Stating Objectives for Classroom Instruction*, 3rd ed (New York : London: Macmillan Pub. Co. ; Collier Macmillan, 1985).

Workshop Activities:

This workshop will consist of three main activities. They work cumulatively to optimize the attendee's understanding of data privacy and advocacy. The first activity will ask participants to work independently and sort out which type of data collection is most interesting to them. The second activity is a collaborative activity; groups are organized by data type (consumer, location, or health). Activity 1 and 2 are about formalizing an understanding of data collection, while Activity 3 is about applying that understanding for political action. Activity 3 will maintain the same groups formed in Activity 2 to further their thoughts on how data and democracy interact.

Activity 1: Introduction to Data Tracking (see Handout 1 in Workshop Materials section below). This activity aligns with Learning Objective 1: Participants will gain an understanding of what data is being collected about them.

The first activity is intended to introduce participants to data tracking. While many of our workshop attendees may have heard that our apps and websites capture our information, it is important to understand exactly what kind of data, the amount of data, and how the information might be used. This activity will allow participants to search for these answers and generate a personal response to it. It will be done individually and will function as a launching point into the rest of the workshop sections. Over the course of the workshop, the types of data we will focus on include consumer data, location data, and health data. For this introductory activity, participants will choose which one interests them most. From there, the workshop instructors will guide them to resources that clarify how the data is captured.

Activity 1/**Choice A: Consumer Data**. If the attendee chooses to look into consumer data, they will be asked to visit these websites:

- Google Ad Data: https://www.google.com/ads/preferences/. This link will direct the attendee to their personal Google account. Assuming their account allows and maintains the "Ad Personalization" option by default, they will be able to see the types of conclusions Google has made based on their online activity, such as their Google searches or activity on Google services (such as Youtube).

- Facebook Ad Data: https://www.facebook.com/ads/preferences. By exploring this link, attendees will be able to see how Facebook shapes advertisements for them based on their activity on Facebook, including their other companies and products like Messenger, Instagram, Facebook Business Tools, etc . Facebook's targeted advertisements could be concluded by what Facebook pages they "like", places where they "check-in" on Facebook, and other information found on their Facebook profile and their friends' profiles.

After searching through these resources, individual attendees should take note of what stands out to them about the data being captured. Instructors will prompt questions like: What stands out to you? Do you feel that the "data double" that Google or Facebook has created for you is accurate? Who is the type of person they are advertising to? Does it matter to you if the online representation is accurate? Why or why not?

Activity 1/**Choice B: Location Data**. If the attendee is interested in how their location data is tracked and used, they will be visiting these resources:

- Google Maps: https://www.androidcentral.com/how-view-your-location-history-google-maps This website provides information on how to view your location history in Google Maps through the "timeline" feature. Through your Google Maps account, Google tracks the places you have visited and the routes you have taken. This feature allows users to browse previous destinations, as the timeline can reach back months or years prior to the discovery and disabling of location tracking.
- iPhone location data: https://www.cultofmac.com/522515/how-to-see-iphone-significant-locations-map/. If an attendee has an iPhone, they are able to view their location history through the Settings app on their device. The steps are: go to settings –> privacy –> location services –> system services –> significant locations –> and choose a city from your history list.

After browsing their location history, attendees should develop a response to how they feel about it and prepare to share what pros/cons they might discover. If they

choose to disable location tracking through their device or Google Maps, they can follow the handout which includes instructions to accomplish this.

Activity 1/**Choice C: Health Data**. Workshop attendees may be interested in how data is captured and used based on their health. This could include data regarding their physical activity, mental health, DNA, and more. For attendees to find out more about how health data can be collected and used, they will browse these resources:

Health Apps:

- "Are Health Apps Putting Your Privacy at Risk?" *Consumer Reports*, March 2019. https://www.consumerreports.org/health-privacy/are-health-apps-putting-your-privacy-at-risk/
- "Patient Privacy at Risk as Health Records Merge with Tech" *Governing*, February 2020, https://www.governing.com/security/Patient-Privacy-at-Risk-as-Health-Records-Merge-with-Tech.html

Genetic Testing:

- "5 biggest risks of sharing your DNA with consumer genetic-testing companies" *CNBC*, June 2018. https://www.cnbc.com/2018/06/16/5-biggest-risks-of-sharing-dna-with-consumer-genetic-testing-companies.html
- "How to use 23andMe without giving up your genetic privacy" *VentureBeat*, September 2013. https://venturebeat.com/2013/09/20/how-to-use-23andme-without-giving-up-your-genetic-privacy/

Regulations:

- "The Access Right, Health Apps, & APIs" *U.S. Department of Health & Human Services*, January 31, 2020. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html
- "eHI and CDT Collaborate to Develop Consumer Privacy Framework for Health Data not Covered by HIPAA"*HIPAA Journal*, February 14, 2020.

https://www.hipaajournal.com/ehi-and-cdt-collaborate-to-develop-consumer-privacy-framework-for-health-data-not-covered-by-hipaa/

After exploring some of these websites, attendees should have a basic understanding of how health information can be used by tech companies. They will be encouraged to share their thoughts on why they chose to look into health data, and if they were surprised to find what they did.

Activity 2 The Impacts of Data Tracking (see Handout 2 in the Workshop Materials section below). This activity aligns with Learning Objective 3: Participants will be able to articulate one data collection issue that concerns them.

The second activity builds upon the individual work completed in Activity 1 and the discussion of Section Two regarding the implications of data tracking. The workshop audience will be divided into groups by data type (consumer data, location data, and health data), but each group will be answering the same set of questions on the handout. The desired result of this activity is for group members to present one key issue relevant to their type of data. They will need to develop why they chose that specific issue and how it might be remedied. The issue that they are able to articulate will later be the basis of Activity 3.

Question 1: What specific kind of data is collected and where does the data come from?

- For consumer data, the groups may discover a wide range of information is collected. This list may include purchase history, credit reporting, debt collection, money transfers, mortgages, student loans, and other types of consumer data.
- For location data collection, this includes mobile device location tracking, GPS data from navigation apps, IP address geolocations, cell phone tower data, ride services, tagged locations etc. It will be helpful to identify certain apps that are known to rely on location data.
- For health data tracking, any data entered for the use of health/fitness apps. This includes a long list of possible data. Groups should provide specific apps and examples.

Question 2: How are users at risk?

- Groups should present possible risks to data collection, such as data being hacked, sold without user consent, used for discrimination, harassment, targeting, etc. Specific examples are encouraged.

Question 3: What authority regulates this kind of data collection?

- Answering this question will be important for continuing onto Activity 3. In order to know how to effectively take steps in ensuring data protection, the person/organization responsible for its regulation must be identified. Depending on the data of focus, the entity responsible could be the UC System, the State Assembly, or the Federal government.

Activity 3 Acting at the Legal and Political Level (see Handout 3 in the Workshop Materials section below). This activity aligns with Learning Objective 4: Participants will be able to strategize ways to connect to and put pressure on public officials and institutions regarding the data collection issue they are concerned with.

The third and final activity is the most important for achieving our workshop goal. The groups will be conducting a brief amount of research in order for them to start an advocacy plan. This activity includes identifying a person to contact and drafting a letter to them regarding the importance of data privacy. This is a practical lesson for attendees who want to start reaching out to political officials and promoting dialogues on data collection regulations.

Step 1: Identify a contact

- Depending on the issue chosen by the group, this contact might be a lawmaker, representative, regent, or other. To search for the best person to contact, browse these resources:
    - Find your California Representative: http://findyourrep.legislature.ca.gov
    - Find your Representatives, learn about bills they have supported, their other political contributions, and get their contact information: https://www.commoncause.org/find-your-representative/
    - List of UC appointed Regents: https://regents.universityofcalifornia.edu/about/members-and-advisors/index.html

        - UCLA Office of the Dean of Students: https://www.deanofstudents.ucla.edu

Step 2: Describe why this contact was chosen

Step 3: Draft a letter to the selected official

- As the final step in this activity, groups should write a letter addressed to their chosen contact. This action plan may then be sent via email, reformatted as a phone call interview, or whatever the preferred approach may be.
- The letter should address very specific concerns or requests. This could include asking them to enforce existing legislation, promote new legislation, close legal loopholes, for accountability for data security advocacy, etc.

Workshop Setting and Formats

The workshop will run for about two hours. It will take place in the Research Commons Classroom of the Charles E. Young Research Library at UCLA. Given the size of the room where the workshop will be held, and the workshop structure and content, the ideal number of participants for this workshop is between twenty and twenty five individuals. We will group participants into clusters of five or six people for various activities. Limiting the number of participants to twenty five will allow us to have enough space in the room and will allow workshop leaders to work closely with each group.

The workshop will have four leaders, which will be the members of the charette group. The workshop will utilize Google Slides and the personal or public, library computing devices. The workshop is contingent on the participants usage of any laptop, mobile phone, or other computing devices, and assumes a minimal level of technological literacy of its participants; there is no specific device requirement, as long as the device has Internet accessibility, as Wifi will be provided courtesy of UCLA. If a participant doesn't have a personal computing device, a laptop can be provided by the library. The workshop content also assumes an intermediate understanding of English from its participants; the workshop material can also be made available online for the participants in an easily translatable format, whether that be into a various languages besides English or into character

vocalization. Finally, Charles E. Young Research Library and the Research Commons classroom within it are both ADA compliant.

Workshop Materials:

See Appendix B

Workshop Budget:

The budget for the workshop will primarily need to cover fair compensation for the instructors, with additional costs for holding the workshop dependent on its location. These depend on access to University resources and the scheduling of the workshop, relative to quarantine recommendations. If University resources cannot be used, some of these costs could be offset with in-kind donations by instructors or other external support, particularly for large expenses such as the meeting space or laptop rentals. We have outlined three scenarios and expected costs below.

Scenario 1: UCLA Library/RC Classroom

Workshop Instructor honorarium	(4)	250/ea1000	
Handout packets of workshop materials	(20)	2.50/ea	50
Promotional flyers	(100)	.25/ea	25
Snacks and drinks			50
Total			**$1125**

Scenario 2: Meeting Space in Westwood

Workshop Instructor honorarium	(4)	250/ea1000	
Handout packets of workshop materials	(20)	2.50/ea	50
Promotional flyers	(100)	.25/ea	25
Snacks and drinks			50
Space rental	(3)	100/hr	300
Laptop rental	(20)	75	1500
Total			**$2925**

Scenario 3: Digital Workshop

Workshop Instructor honorarium	(4)	250/ea1000	
Space rental for instructors	(3)	30/hr	90
Conference software			15
Total			**$1105**

Bibliography

Angwin, Julia and Terry Parris Jr. “Facebook Lets Advertisers Exclude Users by Race.” *ProPublica*. Https://www.propublica.org/. October 28, 2016. https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race.

“Attorney General Ferguson’s Investigation into Premera Data Breach Results in Premera Paying $10 Million Over Failure to Protect Sensitive Patient Data” *Office of the Attorney General*, July 11, 2019, https://www.atg.wa.gov/news/news-releases/attorney-general-ferguson-s-investigation-premera-data-breach-results-premera.

Curran, Dylan. “Are You Ready? This Is All the Data Facebook and Google Have on You” *The Guardian*, March 30, 2018, sec. Opinion. https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy.

Edelman, Gilad. “Can the Government Buy Its Way Around the Fourth Amendment?” *Wired*, February 11, 2020. https://www.wired.com/story/can-government-buy-way-around-fourth-amendment/.

The Editorial Board. “The Government Uses ‘Near Perfect Surveillance’ Data on Americans.” *The New York Times*, February 7, 2020, sec. Opinion. https://www.nytimes.com/2020/02/07/opinion/dhs-cell-phone-tracking.html.

Gronlund, Norman Edward. 1985. *Stating Objectives for Classroom Instruction*. 3rd ed. New York : London: Macmillan Pub. Co. ; Collier Macmillan.

Hill, Kashmir. “The Secretive Company That Might End Privacy as We Know It.” *The New York Times*, January 18, 2020, sec. Technology. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Leigh, Erika. “State Law Sparks Student Debt Controversy.” *ABC Dakota News Now*. December 20, 2017. https://www.dakotanewsnow.com/content/news/State-law-sparks-student-debt-controversy-446255773.html.

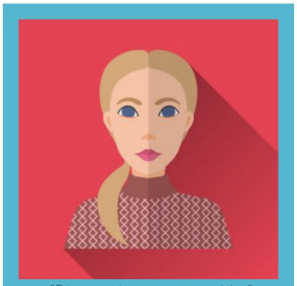
Molla, Rani. “Law Enforcement is Now Buying Cell Phone Location Data from Marketers.” *Vox*. February 7, 2020. https://www.vox.com/recode/2020/2/7/21127911/ice-border-cellphone-data-tracking-department-homeland-security-immigration

Schneier, Bruce. “We’re Banning Facial Recognition. We’re Missing the Point.” *The New York Times*, January 20, 2020, sec. Opinion. https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html.

Warzel, Charlie. “We Need a Law to Save Us From Dystopia.” *The New York Times*, January 21, 2020, sec. Opinion. https://www.nytimes.com/2020/01/21/opinion/facial-recognition-privacy-law.html.

Appendix A: Personas

Mona Abadi - Undergraduate Student



"Discovering a new world ..."

Age: 19
Work: Student
Family: Nuclear Family
Location: Los Angeles, CA
Character: Kind

Curious | Timid | Driven | Caring

Goals

- Graduate with honors and a gain admittance to graduate school
- Effectively navigate all the resources and opportunities at UCLA
- Maintain a strong connection to where she came from (her community, her culture, etc.) and join serve the needs of her community in the future

Frustrations

- Activist at heart, but has limited political power because of status in the United States
- Underserved by her institution and community.
- Has received very limited guidance on how to navigate college and it's numerous resources

Personality

Introvert	Extrovert
Thinking	Feeling
Sensing	Intuition
Judging	Perceiving

Bio

Mona is very excited by all the opportunities available to her at UCLA that weren't before he arrived. She regularly visits the library to check out a laptop, as well as to gain access to various technological tools, which he spends time teaching himself. She is also very newly a regular user of social media, given his new and regular access to the Internet. Mona understands the value of computer literacy and has made increasing her computer literacy a goal during her first year.

She hopes to graduate with honors and hopefully go to graduate school, become a professor, and research the issues within his community and work towards solutions that plague her community.

Motivation

Incentive
Fear
Growth
Power
Social

Brands & Influencers

Preferred Channels

Traditional Ads
Online & Social Media
Referral
Guerrilla Efforts & PR

Amy Lin - Doctoral Student

"Transparency is king"

Age: 29
Work: Teacher's Assistant
Family: Mother, father, older sister
Location: Los Angeles, CA
Character: Driven

Personality

Introvert	Extrovert
Thinking	Feeling
Sensing	Intuition
Judging	Perceiving

Informed | Deliberate | Sophisticated

Goals

- Find a career that puts her technical and analytical expertise to work, while balancing the ethical implications of her work
- Work towards a more equitable future for Teaching Assistants in American universities and colleges
- Empower underrepresented undergraduate students to pursue graduate education
- Continue to develop her technical expertise

Frustrations

- Previous tumultuous career experience as a data entry and analyst specialist
- Many of the viable career options that utilize her highly-demanded skillset at roles that have questionable ethical implications and companies that have business goals and value propositions that don't align with her own

Bio

Amy is a Ph.d candidate in the department of Statistics at UCLA and an inspiring data scientist. She is especially interested in the ethical applications of her studies in industry. She was previously a Data Entry and Analysis Specialist at a Fortune 500 company, were she was forced to grapple with a lot of unfortunate incidents of data breaches. She not only understands all the software and business side of the technical infrastructure that makes technical platforms reliant on data collection for business goals, but also the analytical methods for best analyzing the collected data. Amy also cares deeply about the needs and rights of her fellow workers and is part of a union, where she regularly participates in strikes and other advocacy events.

Motivation

Incentive
Fear
Growth
Power
Social

Brands & Influencers

Preferred Channels

Traditional Ads
Online & Social Media
Referral
Guerrilla Efforts & PR

Jamie Connelly - Non-traditional Undergraduate Student

"For a brighter future"

Age: 31
Work: Student
Family: Married, two kids
Location: Los Angeles, CA
Character: Calculated

Personality

Introvert	Extrovert
Thinking	Feeling
Sensing	Intuition
Judging	Perceiving

Leader | Experimenter | Driven

Goals

- Land a Data Engineering Internship at Google, Microsoft (or any large well-recognized technology company)
- Provide a higher quality of life for his family through the his education and career prospects
- Achieve expert proficiency in specific data visualization tools such as Tableau.

Frustrations

- Balancing full-time student course load with familial responsibilities.
- Tinge of uncertainty regarding the ethics of his future career plans
- Recruiting as a non-traditional student is very difficult given that he doesn't have the educational and professional background some recruiters are looking for

Bio

Jamie is an undergraduate student in the department of Statistics at UCLA and an inspiring data scientist. He returned to school to use his newly acquired education to make a career switch to the lucrative technology industry as a data scientist and better provide for his family. He was previously an active supporter of Andrew Yang, and very much believes that "data is the new oil of the 21st century". While he has the deep understanding of the value of our data, he also has weariness of past controversial events involving personal data usage, Cambridge Analytica in the 2016 U.S. Presidential Election, and how that relates to his future career plans.

Motivation

Incentive
Fear
Growth
Power
Social

Brands & Influencers

Preferred Channels

Traditional Ads
Online & Social Media
Referral
Guerrilla Efforts & PR

Appendix B: Workshop Materials

Your Data & Democracy

HANDOUT 1

While you may have heard about data tracking, what exactly does it mean? Who is tracking my data? How much of my data is captured and sold? What kind of data does this include? These are some of the questions you may be asking about data tracking. This introductory activity is intended to help us start thinking about how we understand data tracking, so we can begin our research and advocacy for data privacy.

Step 1: Before jumping into any online research, what do you already think about data tracking? It is worth considering now, because you may be surprised later. For each statement, fill in the circle depending how true or false you think it is.

STATEMENT:	**TRUE**						**FALSE**
Tech companies buy and sell my personal information	○	○	○	○	○	○	○
I am protected from data tracking as long as I reconfigure my device settings	○	○	○	○	○	○	○
Location services are not recorded and saved by the app	○	○	○	○	○	○	○
My online purchases are only accessible to the company I buy the product from	○	○	○	○	○	○	○
I have legal protection from companies owning my data	○	○	○	○	○	○	○
There are no real-life consequences for tracking people's data	○	○	○	○	○	○	○
Advertisements are targeting me based on my data	○	○	○	○	○	○	○

Step 2: Choose a type of data to research. The options include:

A) Consumer data

B) Location data

C) Health data

Step 3: Follow the instructions on the next page.

Step 4: Debrief with someone next to you about what you found about your data. Was anything you found unexpected? How accurate were your answers in step 1?

Choice A: **Consumer Data**

If you choose to look into consumer data, visit these websites:

- Google Ad Data: https://www.google.com/ads/preferences/
  This link will direct you to your personal Google account. Assuming your account allows and maintains the "Ad Personalization" option by default, you will be able to see the types of conclusions Google has made about you based on your online activity, such as their Google searches or activity on Google services (such as Youtube).
- Facebook Ad Data: https://www.facebook.com/ads/preferences.
  By exploring this link, you will be able to see how Facebook shapes advertisements for you based on your activity on Facebook, including their other companies and products like Messenger, Instagram, Facebook Business Tools, etc . Facebook's targeted advertisements could be concluded by what Facebook pages you "like", places you have "checked-in" on Facebook, and other information found on your Facebook profile and your friends' profiles.
- After searching through these resources, take note of what stands out to you about the data being captured. Do you feel that the "data double" that Google or Facebook has created for you is accurate? Who is the type of person they are advertising to? Does it matter to you if the online representation is accurate? Why or why not?

Choice B: **Location Data**

If you are interested in how location data is tracked and used, visit these resources:

- Google Maps: androidcentral.com/how-view-your-location-history-google-maps.
  This website provides information on how to view your location history in Google Maps through the "timeline" feature. Through your Google Maps account, Google tracks the places you have visited and the routes you have taken. This feature allows users to browse previous destinations, as the timeline can reach back months or years prior to the discovery and disabling of location tracking.
- iPhone location data: https://www.cultofmac.com/522515/how-to-see-iphone-significant-locations-map/. If you have an iPhone, you are able to view your location history through the Settings app on your device. The steps are: go to settings –> privacy –> location services –> system services –> significant locations –> and choose a city from your history list.
- After browsing your location history, develop a response to how you feel about it and prepare to share what pros/cons you have discovered.

Choice C: **Health Data**

You may be interested in how data is captured and used based on your health. This could include data regarding physical activity, mental health, DNA, and more. To find out more about how health data can be collected and used, browse these resources:

- Health Apps:
  - "Are Health Apps Putting Your Privacy at Risk?" Consumer Reports, March 2019. https://www.consumerreports.org/health-privacy/are-health-apps-putting-your-privacy-at-risk/
  - "Patient Privacy at Risk as Health Records Merge with Tech" Governing, February 2020, https://www.governing.com/security/Patient-Privacy-at-Risk-as-Health-Records-Merge-with-Tech.html

- Genetic Testing:
  - “5 biggest risks of sharing your DNA with consumer genetic-testing companies” CNBC, June 2018. https://www.cnbc.com/2018/06/16/5-biggest-risks-of-sharing-dna-with-consumer-genetic-testing-companies.html
  - “How to use 23andMe without giving up your genetic privacy” VentureBeat, September 2013. https://venturebeat.com/2013/09/20/how-to-use-23andme-without-giving-up-your-genetic-privacy/
- Regulations:
  - “The Access Right, Health Apps, & APIs” U.S. Department of Health & Human Services, January 31, 2020. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html
  - “eHI and CDT Collaborate to Develop Consumer Privacy Framework for Health Data not Covered by HIPAA”HIPAA Journal, February 14, 2020. https://www.hipaajournal.com/ehi-and-cdt-collaborate-to-develop-consumer-privacy-framework-for-health-data-not-covered-by-hipaa/
- After exploring some of these websites, you should have a basic understanding of how health information can be used by tech companies. You are encouraged to share your thoughts on why you chose to look into health data, and if they were surprised to find what they did.

Your Data & Democracy

HANDOUT 2

Now that you have done some basic research on one type of data, we will build upon our work in groups. Each group will cover either consumer, location, or health data. Groups will answer the following questions on this handout, and at the end of this activity, groups should have narrowed down their research to a specific concern regarding data tracking.

1) What specific kind of data is collected?
Check all that apply:

- ○ purchase history
- ○ tagged locations
- ○ IP address
- ○ financial loans
- ○ physical activity
- ○ blood type
- ○ money transfers
- ○ cell tower data
- ○ heart rate
- ○ GPS data
- ○ ride service data
- ○ credit score
- ○ medical records
- ○ body measurements
- ○ debt collection

other:

2) Where does the data come from?
Check all that apply:

- ○ debit card transactions
- ○ photos
- ○ wifi connections
- ○ default device settings
- ○ NFC mobile payments
- ○ social media accounts
- ○ data brokers
- ○ audio sources
- ○ voluntarily input

other:

3) Can you link two specific examples together?

4) How are users at risk?

5) What authority regulates this kind of data collection?

Your Data & Democracy

HANDOUT 3

This last activity allows groups to apply our understanding of data tracking to political action. This step is crucial for promoting user data privacy, as the effort needs to reach beyond the individual. Together, groups will draft a letter to the authority who is responsible for the issue they selected in activity 2.

1) Identify a specific contact

- Depending on the issue chosen by the group, this contact might be a lawmaker, representative, regent, or other. To search for the best person to contact, browse these resources:
  - Find your California Representative:
    - http://findyourrep.legislature.ca.gov
  - Find your Representatives, learn about bills they have supported, their other political contributions, and get their contact information:
    - https://www.commoncause.org/find-your-representative/
  - List of UC appointed Regents:
    - https://regents.universityofcalifornia.edu/about/members-and-advisors/index.htmlUCLA Office of the Dean of Students: https://www.deanofstudents.ucla.edu

2) Why was this person chosen?

Discuss among the group why this person is the most suitable to address your concerns about data privacy.

3) Draft a letter to the selected official

- Groups should write a letter addressed to their chosen contact. This action plan may then be sent via email, reformatted as a phone call interview, or whatever the preferred approach may be.
- The letter should address very specific concerns or requests. This could include asking them to enforce existing legislation, promote new legislation, close legal loopholes, for accountability for data security advocacy, etc.
  - Sample letter template:
    - https://www.asbmb.org/advocacy/toolkit/write-a-letter-to-your-legislator

Your Data & Democracy

FUTHER READINGS

Here are some extra readings that relate to the work we did during this workshop:

“Are You Ready? This Is All the Data Facebook and Google Have on You”
article by Dylan Curran: https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy

"Can the Government Buy Its Way Around the Fourth Amendment?"
article by Gilad Edelman: https://www.wired.com/story/can-government-buy-way-around-fourth-amendment/

"Carriers 'Violated Federal Law' By Selling Your Location Data, FCC Tells Congress"
article by Devin Coldewey: https://techcrunch.com/2020/01/31/carriers-violated-federal-law-by-selling-your-location-data-fcc-tells-congress/

"Forget Warrants, Ice Has Been Using Cellphone Marketing Data To Track People At the Border"
article by Rani Molla: https://www.vox.com/recode/2020/2/7/21127911/ice-border-cellphone-data-tracking-department-homeland-security-immigration

"Navigating Patient Data Privacy in the Digital Health Era"
https://lhatrustfunds.com/patient-data-privacy/

"New California Privacy Law May Require Facebook To Completely Change How It Does Business"
article by Gary Guthrie: https://www.consumeraffairs.com/news/new-california-privacy-law-may-require-facebook-to-completely-change-how-it-does-business-021920.html

The New York Times Privacy Project:
https://www.nytimes.com/series/new-york-times-privacy-project

"Terms Of Service: Understanding Our Role in the World Of Big Data"
a comic book about data privacy by Michael Keller and Josh Neufeld:
http://projects.aljazeera.com/2014/terms-of-service/#2

"U.S. Senator Gillibrand Announces Legislation To Create a Data Protection Agency"
https://www.securitymagazine.com/articles/91729-us-sen-gillibrand-announces-legislation-to-create-a-data-protection-agency

"Who Does Google Think I Am?"
a blog post by Greg Boggs: https://www.gregboggs.com/who-does-google-think-you-are/

"Would 'medicare For All' Help Secure Health Data?"
article by Adam Kujawa: https://blog.malwarebytes.com/security-world/2019/11/would-medicare-for-all-help-secure-health-data/