

What ethically significant harms  
and benefits can data present?

*\* based on Introduction to Data Ethics module (Part 1)  
developed by Shannon Vallor, Ph.D.*

# What makes a harm or benefit ethically significant?

- We aim to have a 'good life'.
  - Not just ourselves, but as a society
- Ethically significant harm/benefit happens: "when it has a substantial possibility of making a difference to certain individuals' chances of having a good life, or the chances of a group to live well."
- Ethics implies 'human choice'. **Good intentions** is not enough to make an ethical choice.
- It is not easy to identify the harms and benefits of data in a specific context. We should **increase awareness!**



# What our life interests are?

Data practice can impact all these fundamental interests of human beings.

# Ethically Significant Benefits of Data Practices

# Human Understanding

- We aim to understand the world, how it works to build better technology of the future.
- Complex systems vs smaller systems; we want to understand.
- We can identify (unseen) harms/needs/risks.
  - If we know a minority/marginalized group is being harmed, we may work for the benefit to a wider community.









# Vital Patch


- Real-time health monitoring is a challenging task.
- Understanding such data helps patients to get the necessary treatment.
- Vital Patch, as a data practice, helps many stakeholders.

<https://www.medibiosense.com/vitalpatch/>

**Features**

VitalPatch monitors a total of eight vital signs:

 Single-Lead ECG	 Heart Rate	 Heart Rate Variability	 Respiratory Rate
 Body Temperature	 Body Posture	 Fall Detection	 Activity



The Vital Patch is a health monitoring device in the growing field of Tele-Health. Never before has such a small, elegant device provided so much valuable information for physicians and nurses. This state-of-the-art biosensor monitors eight physiological measurements continuously, in real time. Clinical-grade accuracy without the hassle of traditional monitoring equipment. The best things do come in small packages.



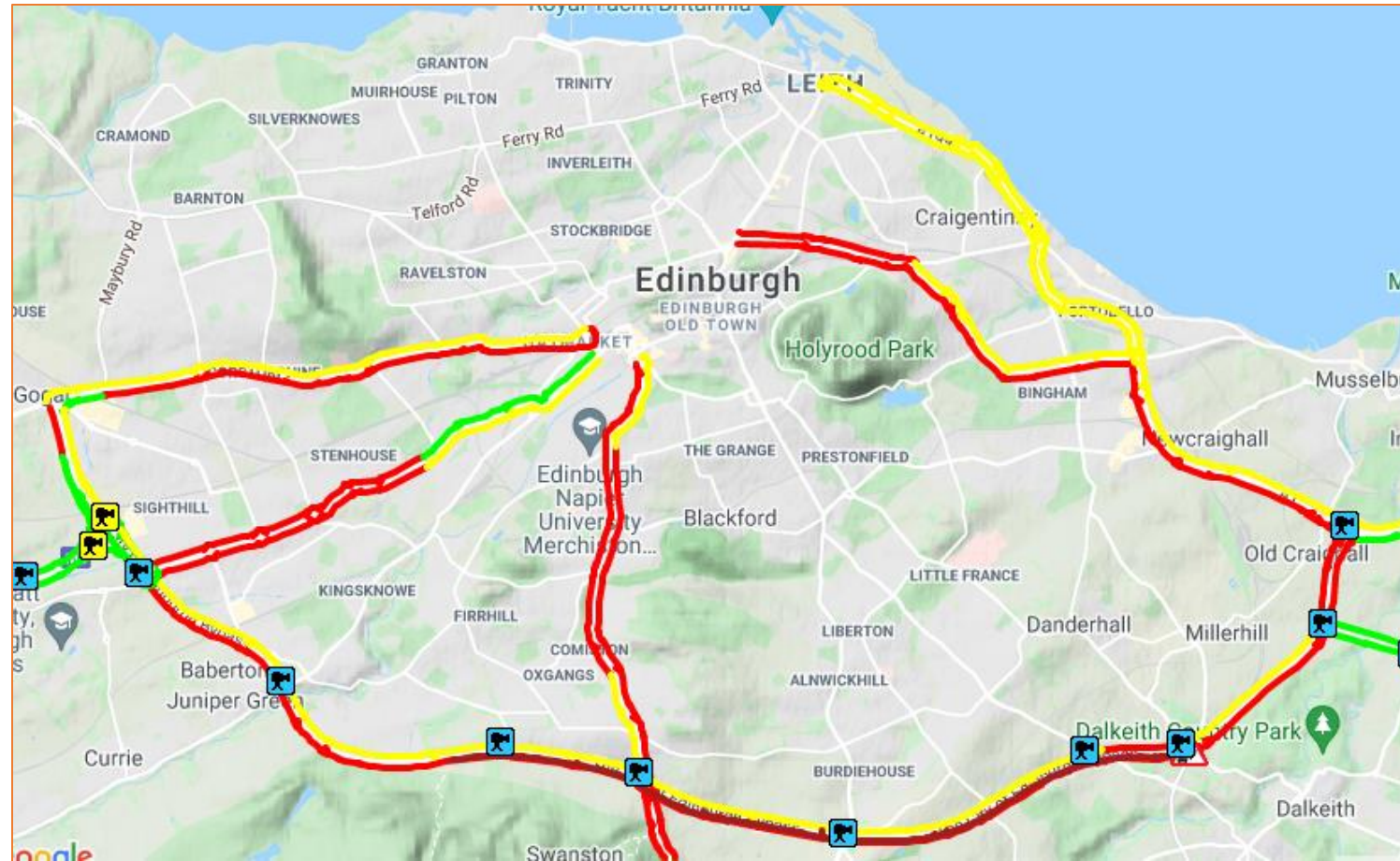
# Social, Institutional and Economic Efficiency

- Understanding -> Improving functioning of the systems
- We use time efficiently to build what we need, while fulfilling goals (social system, policies, humans...)

**In the Vital Patch example, what ethically significant benefits we could think of?**



# Happy people, happy environment...



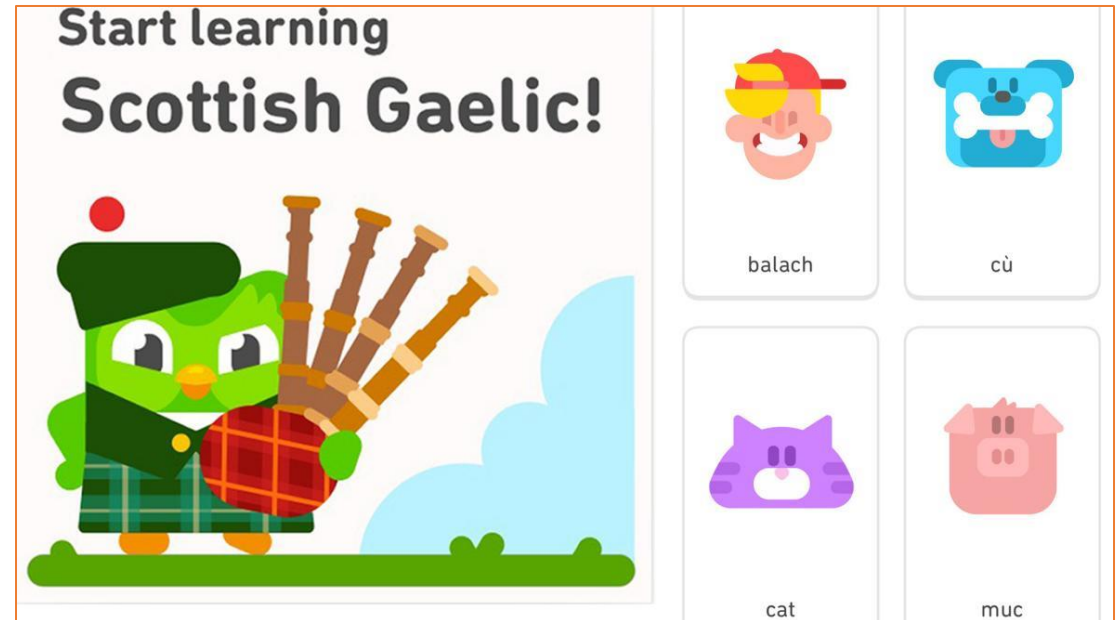


# Predictive Accuracy and Personalization

- We can achieve good outcomes for specific individuals, groups.
- We can provide (real-time) feedback to user inputs.
- Domains: search, ads (cookies), recommender systems, ...
- Data analytics are quite useful here (not everything is AI!!!)
- Context is key -> specific needs and circumstances

# Duolingo

- An AI-based language learning platform.
- They use deep learning algorithms to personalize content.
- It gamifies the learning experience, hence more engagement from the users.



<https://www.duolingo.com/>



# Ethically Significant Harms of Data Practices

# Harms to Privacy & Security

- Everyone generates data.. We share data about ourselves as well as others.
- **Anonymized datasets** can be de-anonymized once merged with other datasets.
- Weakly enforced sets of data regulations and policies protect us from the **reputational, economic** and **emotional harms**.
- Harms can even be fatal (e.g., oppressive regimes).
- Data is also collected by deployed systems (e.g., IoT).

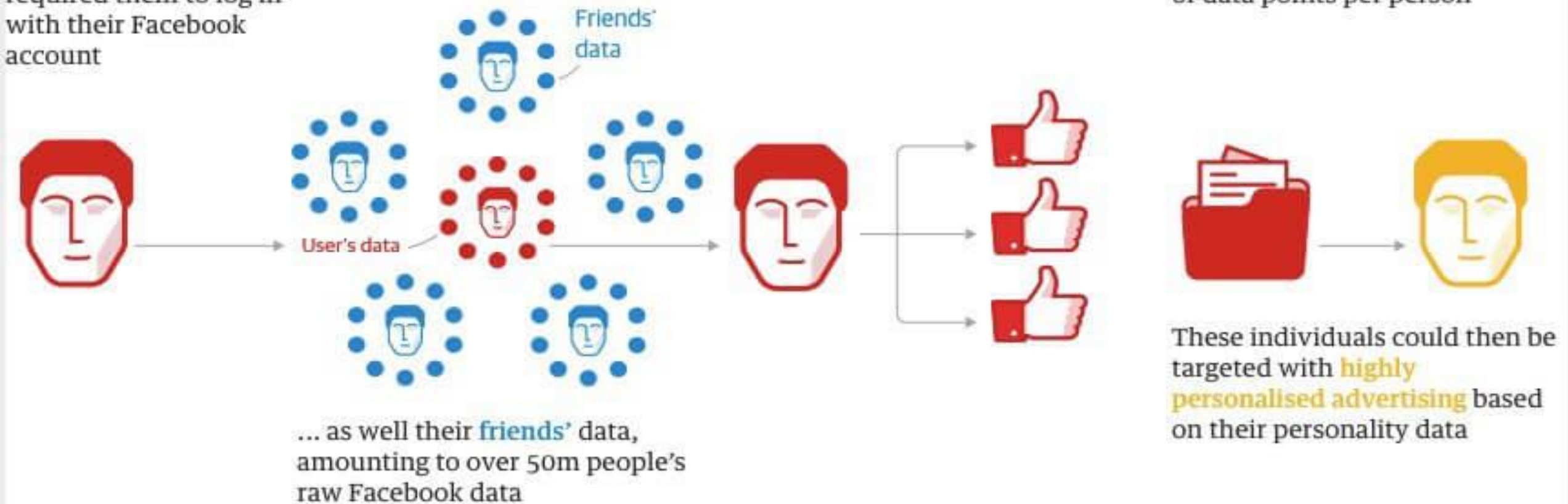
# Cambridge Analytica: how 50m Facebook records were hijacked

**1** Approx. 320,000 US voters ('seeders') were paid \$2-5 to take a **detailed personality/political test** that required them to log in with their Facebook account

**2** The app also **collected data such as likes and personal information** from the test-taker's Facebook account ...

**3** The **personality quiz results** were paired with their Facebook data - such as **likes** - to seek out psychological patterns

**4** Algorithms combined the data with other sources such as voter records to **create a superior set of records (initially 2m people in 11 key states\*)**, with hundreds of data points per person



# Understanding Privacy Violations in Online Social Networks

## Privacy Concerns of Dennis

Dennis wants his friends to see his pictures but not his location.

	No inference	Inference
User	(i) Dennis checks in at a restaurant.	(iii) Dennis shares a picture without declaring his location. It turns out that his picture is geo-tagged.
Others	(ii) Charlie shares a picture with everyone. He tags Dennis in it as well.	(iv) Charlie checks in at a restaurant. At the same time, Dennis shares a picture of Charlie.



# Real Life Scenarios from Online Social Networks

The image shows a screenshot of a social media post and an article snippet. The social media post is from a user named 'Claudy' and is titled 'Vodka Shots'. The post content is partially obscured by a redacted area, but the visible text includes 'OMG I HATE MY JOB!! My b...', 'always making me do shit stuff just to p...', and 'Yesterday at 18:03 · Comment · Like'. Below the post, there are two comments: one from 'Terry' asking 'Hold up aren't you babysitting?????' and another from 'Claudy' replying 'Yes'. The article snippet is titled 'Celebrities' Photos, Videos May Reveal Location' and is dated July 16, 2010. The author is 'KI MAE HEUSSNER'. The article text discusses how celebrities might unintentionally reveal their locations through photos uploaded to the Internet, making them vulnerable to tech-savvy thieves and unwanted visits by starstruck fans.

Our online survey with 330 participants shows that more than 90% of privacy violations occur through inference.

# Privacy in Internet-of-Things Era

## Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance

Julia Bernd

*International Computer Science Institute  
University of California, Berkeley*

Ruba Abu-Salma

*Centre INRIA Sophia Antipolis-Méditerranée*

Alisa Frik

*International Computer Science Institute  
University of California, Berkeley*

### Abstract

The increasing use of smart home devices affects the privacy not only of device owners, but also of individuals who did not choose to deploy them, and may not even be aware of them. Some smart home devices and systems, especially those with cameras, can be used for remote surveillance of, for example, domestic employees. Domestic workers represent a special case of bystanders' privacy, due to the blending of home, work, and care contexts, and employer-employee power differentials. To examine the experiences, perspectives, and privacy concerns of domestic workers, we begin with a case study of nannies and of parents who employ nannies. We conducted 26 interviews with nannies and 16 with parents. This paper describes the research agenda, motivation, and methodology for our study, along with preliminary findings.

for domestic employees or service workers. may affect the nature of the individual relationships between those employees/service workers and their employers, as well as reflecting or amplifying general social dynamics.

Our first case study focuses on nannies, and also on time babysitters. Our decision to begin with these relationships, rather than with other types of domestic workers, is based on several motivations. First, by analysing employment relationships, we hope to shed light on the interplay of socio-economic power differentials and privacy concerns, and how we can reduce the effects of those differentials. Second, most research on privacy concerns, at least in the academic literature, focuses either on primary end users of technology, or else on general public surveys, where data subjects have no connection to the technology decision-makers. Domestic workers present

## Owning and Sharing: Privacy Perceptions of Smart Speaker Users

NICOLE MENG, University of Edinburgh, UK

DILARA KEKÜLLÜOĞLU, University of Edinburgh, UK

KAMI VANIEA, University of Edinburgh, UK

Intelligent personal assistants (IPA), such as Amazon Alexa and Google Assistant, are becoming increasingly present in multi-user households leading to questions about privacy and consent, particularly for those who do not directly own the device they interact with. When these devices are placed in shared spaces, every visitor and cohabitant becomes an indirect user, potentially leading to discomfort, misuse of services, or unintentional sharing of personal data. To better understand how owners and visitors perceive IPAs, we interviewed 10 in-house users (account owners and cohabitants) and 9 visitors from a student and young professionals sample who have interacted with such devices on various occasions. We find that cohabitants in shared households with regular IPA interactions see themselves as owners of the device, although not having the same controls as the account owner. Further, we determine the existence of a smart speaker etiquette which doubles as trust-based boundary management. Both in-house users and visitors demonstrate similar attitudes and concerns around data use, constant monitoring by the device, and the lack of transparency around device operations. We discuss interviewees' system understanding, concerns, and protection strategies and make recommendation to avoid tensions around shared devices.

# Harms to Fairness and Justice (i)

- We want to be judged and treated fairly (government, work, education, healthcare, finance and so on)
- Biases that rest on falsehoods, sampling errors, and unjustifiable discriminatory practices are **very common** in data practices.
- **Implicit** data biases are the most difficult ones to spot!
- **Proxies** can still be indicators of protected features such as race, gender etc. (e.g., zip code -> indicator of race or income).

# Harms to Fairness and Justice (ii)

- The harms can also be driven by:
  - Poor quality, mislabeled, error-riddled data
  - Inadequate design and testing of data analytics
  - Lack of training/auditing
- Some groups are affected by such data practices, and they **lose their chance** to live a 'good life' for no good reasons...
- Some potential harms:
  - Economic devastation
  - Psychological, reputational and health damage
  - The loss of physical freedom
  - ...

# Pitfalls of Artificial Intelligence Decisionmaking Highlighted In Idaho ACLU Case



By [Jay Stanley](#), Senior Policy Analyst, ACLU Speech, Privacy, and Technology Project

JUNE 2, 2017 | 1:30 PM

TAGS: [Privacy & Technology](#)



- Disadvantaged group: 4000 Idahoans with developmental and intellectual disabilities
- The amount of assistance that they were being given by Medicaid program was being suddenly cut by 20 or 30 percent. An investigation takes place.
- It turns out that a magic Excel formula computes scores based on responses collected during an assessment review.
- They spend \$50000 to test the system to understand the workings of the system.
- Many flaws detected: bad quality of data, partial use of historical data, incorrect statistics....

# Harms to Transparency and Autonomy

- What is **transparency**?
  - It is the ability to see how a given social system or institution works.
  - The focus is on understanding the outcome: "**Why?**"
- What is **autonomy**?
  - It is the ability to govern or steer the course of one's life.
  - The focus is on **control**.
  - In the AI context, autonomy refers to an agent making decisions on its own. (e.g., fully-, semi-automated agents)
- Autonomy ~ chances for a good life depend on you!



# Example: Self-driving cars

## **Self-driving Uber car involved in fatal accident in Arizona**

It's believed to be the first pedestrian fatality attributed to a self-driving vehicle.



<https://www.nbcnews.com/tech/innovation/self-driving-uber-car-involved-fatal-accident-arizona-n857941> (March 2018)

# Why lack of transparency is a problem?

- AI systems can make life-affecting decisions (e.g., loan application)
  - Risk factor: Big Data, Complex Data, Machine Learning Algorithms...
  - Explanations may be limited, which **restrict autonomy**.
- Intellectual property rights and social transparency should be appropriately **balanced**.
  - Proprietary technology makes it difficult to be transparent sometimes. The courts will decide in some cases (e.g., Idaho case)
- Data practices should **take an ethically appropriate measure** of social transparency (e.g., public discussion and negotiation). They impact the quality of people's lives.

# Summary

- Ethically Significant Benefits:
  - We can identify the problems better to build intelligent software.
  - We can offer users a personalized experience based on their needs.
- Ethically Significant Harms:
  - Security & Privacy harms happen widely online.
  - Implicit/explicit biases lead to inaccurate and unjust decisions.
  - Lack of transparency takes away the user's autonomy, hence their chances to live a good life.

# Case Study

- Now we are ready to think about Case Study 1 (page 13) in the following book:

An Introduction to Data Ethics by Shannon Vallor:

<https://www.scu.edu/media/ethics-center/technology-ethics/IntroToDataEthics.pdf>