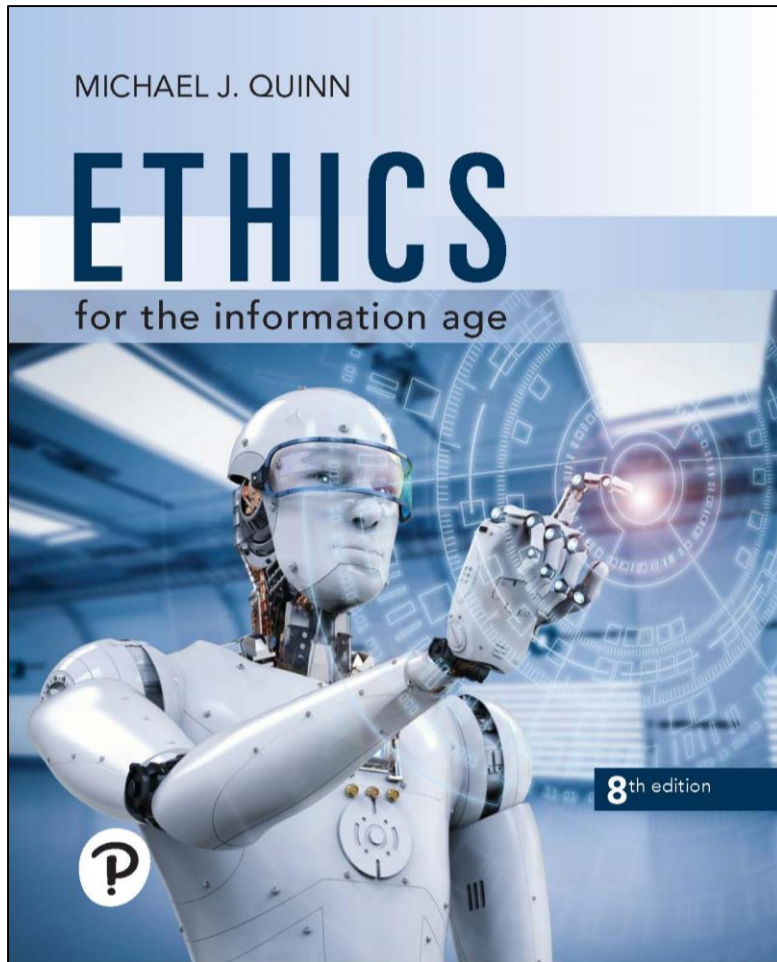


# Ethics for the Information Age

Eighth Edition



## Chapter 5

### Information Privacy

# Learning Objectives

**5.1** Introduction

**5.2** Perspectives on privacy

**5.3** Information disclosures

**5.4** Data mining

**5.5** Examples of consumer or political backlash

# 5.1 Introduction

# Information Technology Erodes Privacy

- Computers, databases, and Internet enable ever-improving information
  - collection
  - exchange
  - combination
  - distribution
- Easier than ever to get information about others, including **total strangers**
- Scott McNealy: “You have zero privacy anyway. Get over it.”
- **Is privacy important? If so, can we protect it?**

# Themes of This Chapter

- What is privacy? Do we have a **natural right to privacy**?
- Tension between **right to privacy** and need to be able to **know enough about others** to trust them
- How organizations collect information about our daily activities
- How profiles of individuals are created through data mining
- How marketers benefit from having profiles of consumers
- Techniques now being extended to realm of **politics**

## 5.2 Perspectives on Privacy

# Defining Privacy

- Privacy related to notion of **access**
- **Access**
  - Physical proximity to a person
  - Knowledge about a person
- Privacy is a “zone of inaccessibility”
- **Privacy violations are an affront to human dignity**
- **Too much individual privacy can harm society**
- **Where to draw the line?**

# Harms of Privacy

- Can be a **cover** for **illegal** or **immoral** activities
- Can be a burden on the nuclear family
- Can hide dysfunctional families
- People on society's fringes can be ignored



# Benefits of Privacy

- Necessary for each individual's **growth as a unique person**
- Signals that individuals are responsible for themselves
- Recognizes everyone's true freedom
- Lets people be themselves
- Allows people to shut out world so they can focus, be creative, and grow intellectually and spiritually
- Fosters the development of loving, trusting, caring, intimate relationships

# Privacy and Trust

- Perhaps modern life is actually more private than life centuries ago
  - Most people don't live with extended families
  - Automobile allows us to travel alone
  - Television (& phone) v. public entertainment (Cinema, Theater)
- Challenge: we now live among strangers
- Remedy: establishing reputations
  - Ordeal, such as lie detector test or drug test
  - Credential, such as driver's license, key, ID card, college degree
- **Establishing reputation is done at the cost of reducing privacy**

# Case Study: New Parents

- Sullivans have a baby girl
- Both work; they are concerned about performance of full-time **nanny**
- Purchase program that allows monitoring through laptop's **camera** placed in family room
- They **do not inform nanny** she is being monitored

# Rule Utilitarian Evaluation

- If everyone monitored nannies, it would not remain a secret for long
- Consequences
  - Nannies would be on best behavior in front of camera
  - Might **reduce child abuse** and parents' peace of mind
  - Would also **increase stress** and **reduce job satisfaction** of child care providers
  - Might result in **higher turnover rate** and less experienced pool of nannies, who would provide **lower-quality care**
- **Harms** appear greater than **benefits**, so we conclude action was **wrong**

# Kantian Evaluation

- Imagine rule, “An employer may secretly monitor the work of an employee who works with vulnerable people”
- **If universalized**, there would be no expectation of privacy by employees, so secret monitoring would be impossible
- Proposed rule is **self-defeating**, so it is **wrong** for Sullivans to act according to the rule

## 5.3 Information Disclosures

# Public Records

- Public record: information about an incident or action reported to a government agency for purpose of informing the public
- Examples: birth certificates, marriage licenses, motor vehicle records, criminal records, deeds to property
- Computerized databases and Internet have made public records much easier to access

# Information Held by Private Organizations

- Credit card purchases
- Purchases made with **loyalty cards**
- Voluntary disclosures
- **Posts to social network sites**



# Data Gathering and Privacy Implications

- Facebook tags
- Enhanced 911 services
- Rewards or loyalty programs
- Implanted chips
- Mobile apps
- Facebook Login
- OnStar (location notify)
- Automobile “black boxes”
- Medical records
- Digital video recorders
- Cookies

# Facebook Tags

- Tag: Label identifying a person in a photo
- Facebook allows users to tag people who are on their list of friends
- About 100 million tags added per day in Facebook
- Facebook uses facial recognition to suggest name of friend appearing in photo
- Does this feature increase risk of improper tagging?

# Enhanced 911 Services

- Cell phone providers in United States required to track locations of active cell phones to within 100 meters
- Allows emergency response teams to reach people in distress
- What if this information is sold or shared?

# Rewards or Loyalty Programs

- Shoppers who belong to store's rewards program can save money on many of their purchases
- Computers use information about buying habits to provide personalized service
  - ShopRite computerized shopping carts with pop-up ads
- **Do card users pay less, or do non-users get overcharged?**

# Implanted Chips

- Taiwan: Every domesticated dog must have an implanted microchip
  - Size of a grain of rice; implanted into ear
  - Chip contains name, address of owner
  - Allows lost dogs to be returned to owners
- RFID tags approved for use in humans
  - Can be used to store medical information
  - Can be used as a “debit card”

# Mobile Apps

- Many apps on Android smartphones and iPhones collect location information and sell it to advertisers and data brokers
  - Angry Birds
  - Brightest Flashlight
- Flurry: a company specializing in analyzing data collected from mobile apps
  - Has access to data from > 500,000 apps

# Facebook Login

- Allows people to login to Web sites or apps using their Facebook credentials
- App's developer has permission to access information from person's Facebook profile: name, location, email address, and friends list

# OnStar (GM)

- OnStar manufactures communication system incorporated into rear-view mirror
- Emergency, security, navigation, and diagnostics services provided to subscribers
- Two-way communication and GPS
- Automatic communication when **airbags** deploy
- Service center can even disable gas pedal



# Automobile “Black Boxes”

- Modern automobiles come equipped with **Event Data Recorder (EDR)**a “black box” –remember plane Bbox!
- Maintains data for five seconds:
  - Speed of car
  - Amount of pressure being put on brake pedal
  - Seat belt status
- After an accident, investigators can retrieve and gather information from the “black box”



# Medical Records

- Advantages of changing from paper-based to electronic medical records
- Quicker and cheaper for information to be shared among caregivers
  - Lower medical costs
  - Improve quality of medical care
- Once information in a database, more difficult to control how it is disseminated

# Digital Video Recorders

- TiVo service allows subscribers to record programs and watch them later (1999)
- TiVo collects detailed information about viewing habits of its subscribers
- Data collected second by second, making it valuable to advertisers and others interested in knowing viewing habits

# Cookies

- Cookie: File placed on computer's hard drive by a Web server
- Contains information about visits to a Web site
- Allows Web sites to provide personalized services
- Put on hard drive without user's permission
- You can set Web browser to alert you to new cookies or to block cookies entirely

# General Data Protection Regulation

- General Data Protection Regulation (GDPR): set of rules governing collection of information from citizens of **European Union**
- **Requires companies to...**
  - Disclose **information** they are seeking **to collect**
  - Disclose **why** they are collecting it
  - **Get permission** before collecting it
- Responding to GDPR, most large American companies are adopting new privacy guidelines
  - Web-site banners informing users, asking for consent

# 5.4 Data Mining

# Data Mining Defined

- Searching records in one or more databases, looking for **patterns or relationships**
- Can be used to create profiles of individuals
- Allows companies to build more personal relationships with customers

# Google's Personalized Search

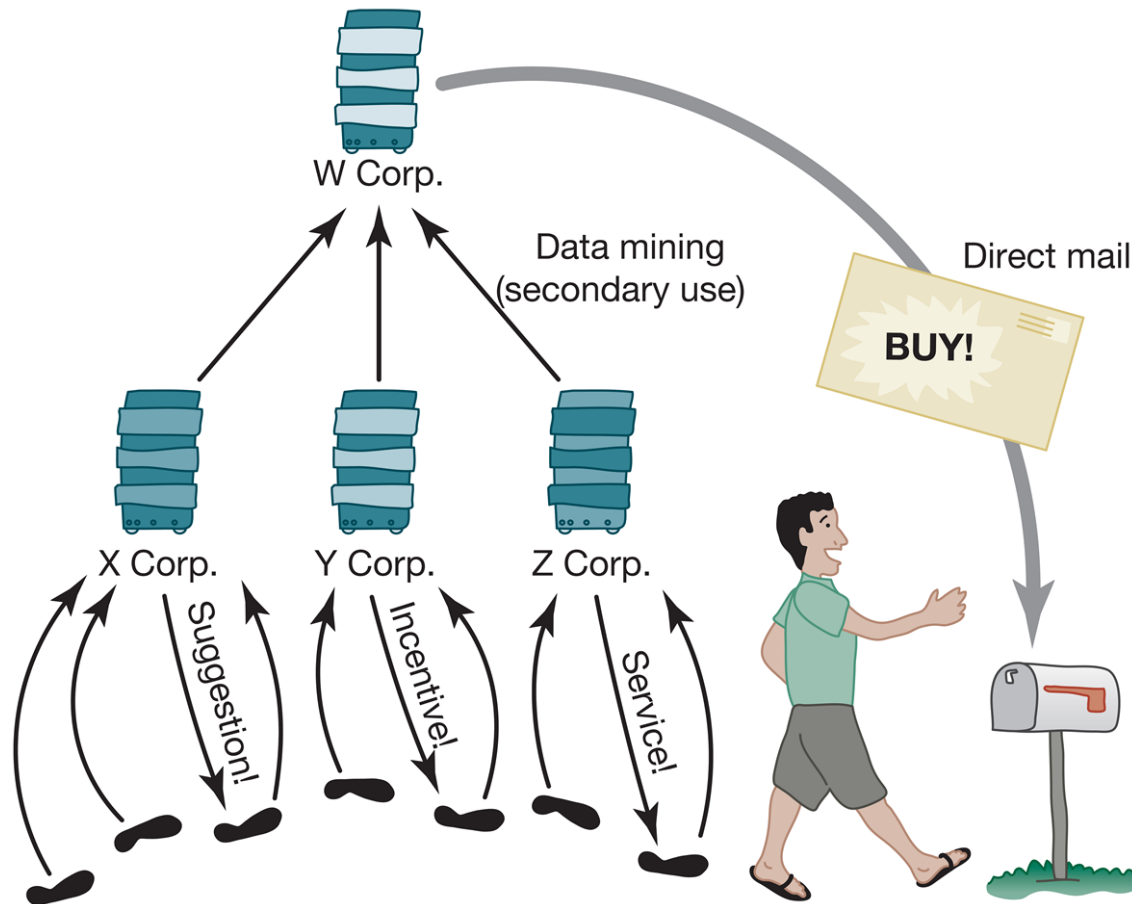
- Secondary use: Information collected for one purpose use for another purpose
- Google keeps track of your search queries and Web pages you have visited
  - It uses this information to infer your interests and determine which pages to return
  - Example: “bass” could refer to fishing or music
- Also used by retailers for direct marketing



# Limiting Information Google Saves

- You can limit amount of information Google saves about your activities
- Privacy Checkup lets you pause collection of personal information
  - Search queries and other Google activity
  - Location information collected from signed-in devices
    - Where you have gone
    - How often you have gone there
    - How long you have stayed
    - Customary routes of travel
  - Contact and calendar information
  - Recordings of your voice and accompanying audio
  - YouTube search queries
  - YouTube videos you have watched

# Secondary Uses of Information



# Collaborative Filtering

- Form of data mining
- Analyze information about preferences of **large number** of people to predict what **one person** may prefer
  - Explicit method: ask people to rank preferences
  - Implicit method: keep track of purchases
- Used by online retailers and movie sites

# Ownership of Transaction Information

- Who controls transaction information?
  - Buyer?
  - Seller?
  - Both?
- **Opt-in:** Consumer must explicitly give permission before the organization can share info
- **Opt-out:** Organization can share info until consumer explicitly forbid it
- Opt-in is a barrier for new businesses, so direct marketing organizations prefer opt-out

# “Target”-ing Pregnant Women

- Most people keep shopping at the same stores, but new parents have malleable shopping habits
- Targeting pregnant women a good way to attract new customers
- Target did data mining to predict customers in second trimester of pregnancy
  - Large amounts of unscented lotion, extra-large bags of cotton balls, nutritional supplements
- Mailings included offers for unrelated items with offers for diapers, baby clothes, etc.

# Credit Reports

- Example of how information about customers can itself become a commodity
- Credit bureaus
  - Keep track of an individual's assets, debts, and history of paying bills and repaying loans
  - Sell credit reports to banks, credit card companies, and other potential lenders
- System gives you more choices in where to borrow money
- Poor credit can hurt employment prospects

# Targeted Direct Mail

- Businesses mail advertisements only to those most likely to purchase products
- Data brokers provide customized mailing lists created for information gathered online and offline
- Example of making inferences for targeted direct mail
  - Shopping for clothes online + frequent fast-food dining + subscribing to premium cable TV channels → more likely to be obese
- Two shoppers visiting same site may pay different prices based on inferences about their relative affluence

# Microtargeting

- Political campaigns determine voters most likely to support particular candidates
  - Voter registration
  - Voting frequency
  - Consumer data
  - GIS data
- Target direct mailings, emails, text messages, home visits to most likely supporters



# Spamming

- Transmission of the same e-mail message to a large number of people
- Extremely inexpensive method of marketing
- Used by many legitimate organizations
- Can contain unwanted and objectionable materials

# Spamming (continued)

- When is it OK to spam?
  - Spammers cannot disguise their identity
  - There must be a label in the message specifying that the e-mail is an ad or solicitation
  - They must include a way for recipients to indicate they do not want future mass mailings

# Social Network Analysis

- Collect information from social networks to inform decisions
- Police use Facebook and Twitter posts to deploy officers on big party nights
- Banks combine social network data with credit reports to determine creditworthiness
- May analyze twitter data to predict crime/suicide and deploy police/help

# Controlling Your Facebook Info (1 of 2)

- You can change your Facebook settings to minimize who can see what you're doing
- Privacy settings
  - Who can see your friends list?
  - Who can see your future posts?
  - Who can look you up using your email address?
  - Who can look you up using your phone number?
  - Do you want search engines to link to your profile?
  - Limit audience for posts you've shared?

# Controlling Your Facebook Info (2 of 2)

- Timeline and Tagging
  - Who sees tag suggestions when photos look like you?
  - Review posts you're tagged in?
  - Review tags people add to your posts?
- Location History
- Ads – Based on
  - Relationship status
  - Employer
  - Job title
  - Education
  - Data from partner
  - Activity on Facebook Company Products
  - Social actions

# Netflix Prize

- Netflix offered \$1 million prize to any group that could come up with a significantly **better algorithm for predicting user ratings** (2006)
- Released more than **100 million movie ratings** from a half million customers
  - Stripped ratings of private information
- **Researchers demonstrated that ratings not truly anonymous if a little more information from individuals was available**
- U.S. Federal Trade Commission complaint and lawsuit
- Netflix canceled sequel to Netflix Prize (2010)

# AOL Search Dataset

- AOL researcher **Dr. Chowdhury** posted three months' worth of user **queries from 650,000 users** (2006)
- No names used; random integers used to label all queries from particular users
- **Researchers identified some users from queries; e.g. many people performed searches on their own names**
- New York Times investigation led to public outcry
- AOL took down dataset, but already copied and reposted
- **AOL fired Dr. Chowdhury and his supervisor**

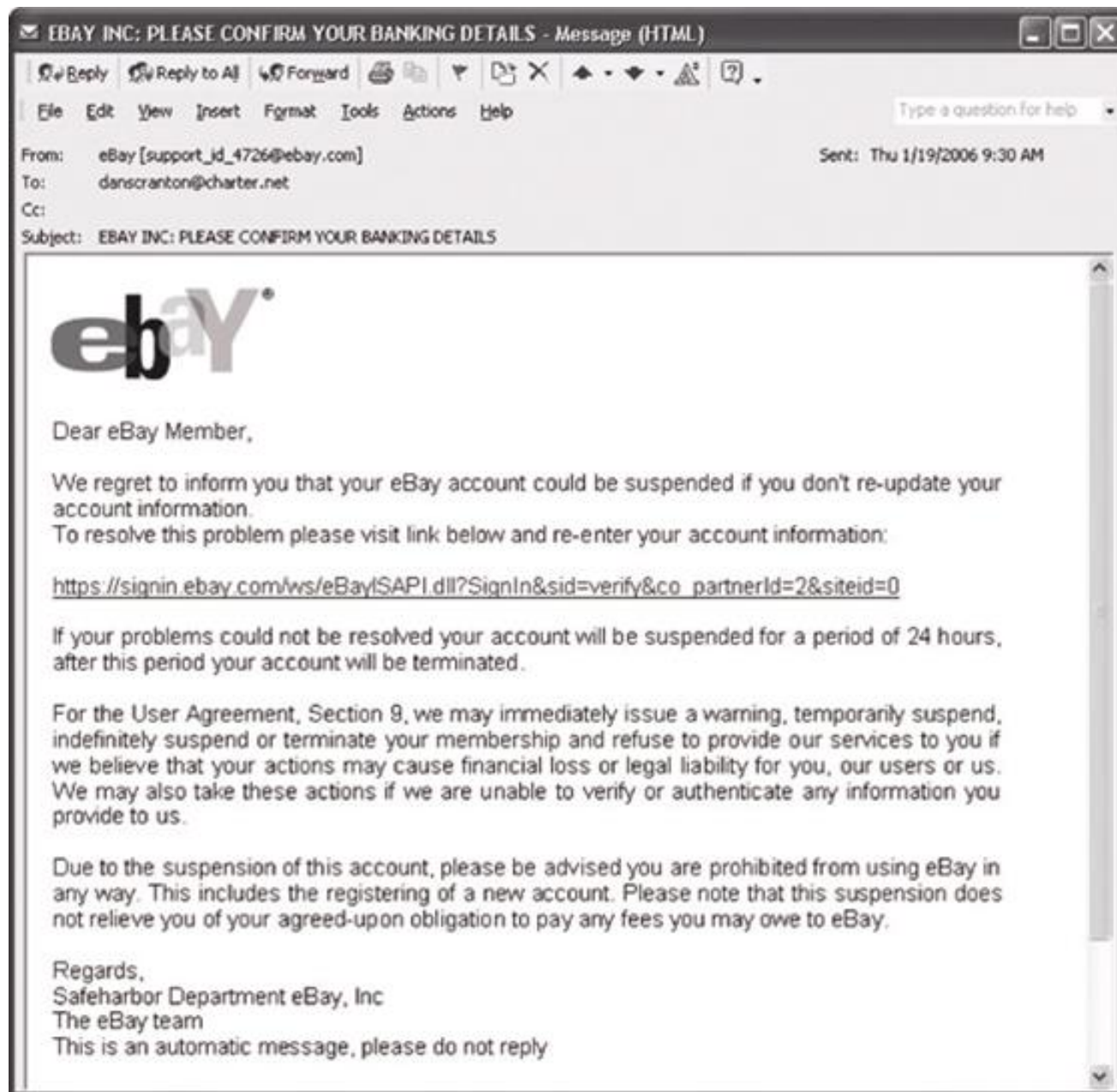
# Identity Theft

- Theft of key pieces of personal information to gain access to a person's financial accounts
- Information includes:
  - Name
  - Address
  - Date of birth
  - Social Security number
  - Passport number
  - Driver's license number
  - Mother's maiden name



# Identity Theft (continued)

- Phishing
  - Attempt to steal personal identity data
  - By tricking users into entering information on a counterfeit Web site
  - Spear-phishing - a variation in which employees are sent phony e-mails that look like they came from high-level executives within their organization
  - Example:



# Identity Theft (continued)

- Spyware
  - Keystroke-logging software
  - Enables the capture of:
    - Account usernames
    - Passwords
    - Credit card numbers
    - Other sensitive information
  - Operates even if an infected computer is not connected to the Internet

## 5.5 Examples of Consumer or Political Backlash

# Marketplace: Households

- Lotus Development Corporation developed CD with information on 120 million Americans
- Planned to sell CD to small businesses that wanted to create mailing lists based on various criteria, such as household income
- More than 30,000 consumers complained to Lotus about invasion of privacy
- Lotus **dropped plans** to sell CD

# Facebook Beacon

- 2007: Facebook announced **Beacon**, a targeted advertising device
  - Facebook user makes purchase
  - Facebook broadcasts purchase to user's friends
  - Based on **opt-out** policy: users enrolled unless explicitly asked to be excluded
- A significant source of advertising revenue for Facebook
- MoveOn.org led online campaign lobbying Facebook to switch to an **opt-in** policy
- Mark **Zuckerberg apologized**, and Facebook **switched to an opt-in** policy

# Malls Track Shoppers' Cell Phones

- In 2011 two malls recorded **movement of shopper** by tracking locations of cell phones
  - How much time people spend in each store?
  - Do people who shop at X also shop at Y?
  - Are there unpopular areas of mall?
- Small signs informed shoppers of study
- After protest, mall quickly halted study

# iPhone Apps Upload Address Books

- In 2012 a programmer discovered **Path** was uploading iPhone address books without permission
- Internet community pointed out this practice violated Apple's guidelines
- CEO of **Path** apologized; app rewritten
- Twitter, Foursquare, and Instagram also implicated for same practice



# Instagram's Proposed Change to Terms of Service

- Late 2012: Instagram announced changes
  - Privacy policy
  - Terms of service
- Legal experts: Instagram and Facebook would have right to **use photos in ads without permission**
- Instagram CEO: New policy misunderstood
- Changed advertising section of terms of service agreement back to original version

# Cambridge Analytica (1 of 3)

- Robert Mercer's vision: **Use data analytics to help conservative candidates and causes**
- Mercer formed joint venture with SCL Group and invested \$15 million in new firm: Cambridge Analytica
- SCL Group **hired Aleksandr Kogan** to gather data about American voters
- Kogan created survey app: "thisisyourdigitallife"
  - Promoted survey using Amazon's **Mechanical Turk**
  - Users paid \$1 or \$2 to take personality test
  - Users had to access app using **Facebook Login**
  - Users agreed that app would **download information about them and their Facebook friends**

# Cambridge Analytica (2 of 3)

- Personal data collected from **270,000** people who took surveys and as many as **87 million** people who were on their friends' lists
- **Kogan shared profiles with Cambridge Analytica**
- About 30 million profiles were detailed enough that Cambridge Analytica could combine data with other data they had, creating psychographic profiles
  - Classified voters over five personality traits: **openness** الانفتاح, **conscientiousness** الضمير, **extroversion** الانبساط, **agreeableness** القبول, **neuroticism** العصابية
  - Strategy: target ads based on psychographic profile
- Ted Cruz campaign hired Cambridge Analytica to help with microtargeting
  - Value of advice debatable
  - Campaign staffers said **predictions were bad**

# Cambridge Analytica (3 of 3)

- Trump campaign hired Cambridge Analytica in fall 2016 – **firm promised to provide names of millions of voters likely to vote for Trump**
- “Data breach” story broke in spring 2018
  - Facebook response
    - Not a breach – everyone who used Kogan’s app had granted their consent, and privacy settings of their friends allowed their information to be shared
    - Kogan had perpetrated a fraud by sharing data with Cambridge Analytica
    - **Suspended accounts of Kogan and Cambridge Analytica**
  - Mark Zuckerberg called to Washington, DC, and testified for 10 hours in front of two Congressional Committees
- May 2018: **Cambridge Analytica filed for bankruptcy**

# NSO/Pegasus

- spyware Pegasus
- Remote zero-click surveillance of smartphones.
- Founded in 2010
- NSO **Claim**: provide **authorized governments** with technology that helps them combat terror and crime: But
- Human rights/government abuse made the headlines
- October 2019: WhatsApp and Facebook sued NSO under the US Computer Fraud and Abuse Act (CFAA)
- November 3, 2021: Boycotted by US
- November 23, 2021: Apple sues NSO

# Summary

- Modern information technology makes it much easier to collect and transmit information
- Privacy a balancing act
  - Desires of individuals
  - Profit motives of companies
  - Common good
- Public records: information that communities have decided should be known to all
- Sometimes must share personal information to get something we want
  - Disclose income tax statements to get a home loan
- Companies collect more information to market more selectively – some have pushed the boundaries of what society will tolerate

# Copyright



**This work is protected by United States copyright laws and is provided solely for the use of instructors in teaching their courses and assessing student learning. Dissemination or sale of any part of this work (including on the World Wide Web) will destroy the integrity of the work and is not permitted. The work and materials from it should never be made available to students except by instructors using the accompanying text in their classes. All recipients of this work are expected to abide by these restrictions and to honor the intended pedagogical purposes and the needs of other instructors who rely on these materials.**