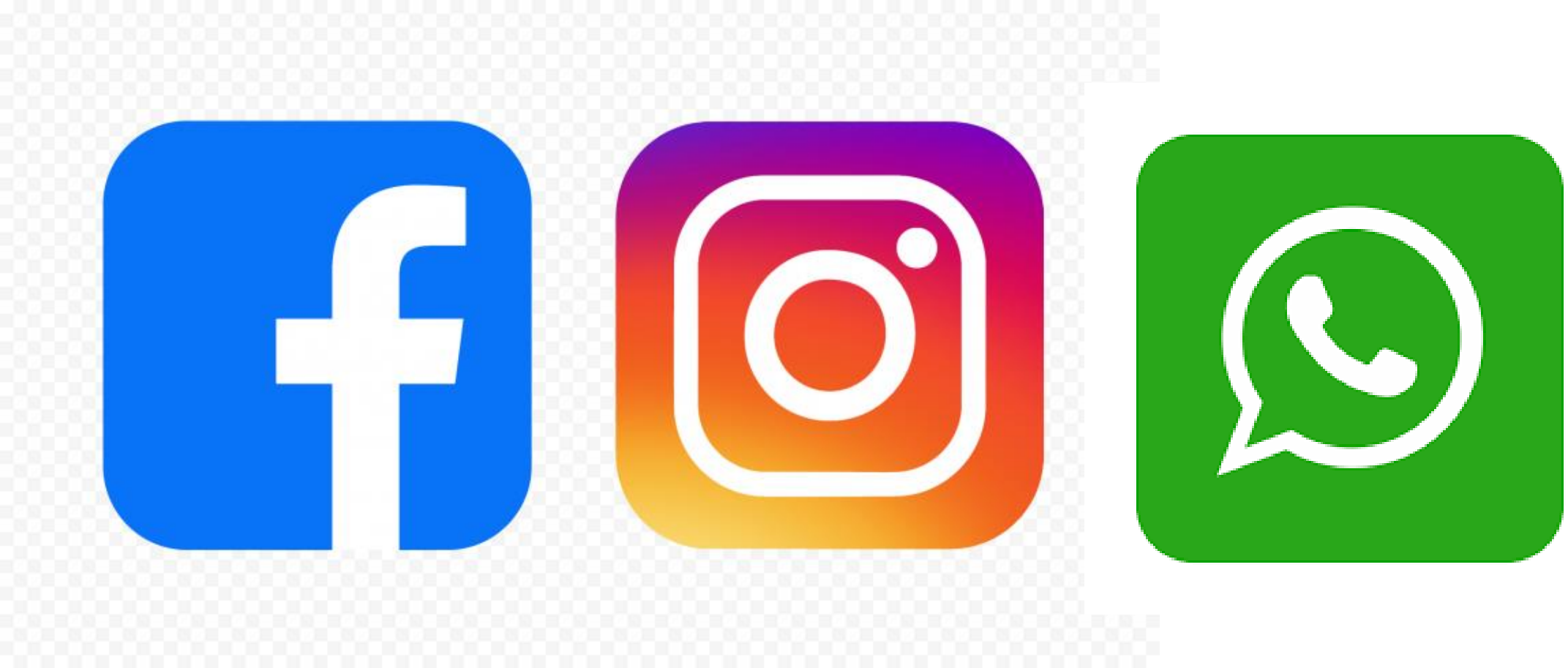
Privacy

Ifeoma Adaji

What caused yesterday's social media outage?



Learning objectives

- Define privacy
- List threats to privacy
- Describe the risks to privacy that come with new technology
- Explain the risks associated with privacy
- List fair information principles
- Explain the 2 aspects of privacy in social networks
- Describe privacy policies in Canada, EU and US

Privacy

- Freedom from intrusion – being left alone
- Control of information about oneself
- Freedom from surveillance (from being followed, tracked, watched and eavesdropped upon?
- Can we truly expect complete privacy?
  - Others may initiate conversation
  - We can't always control information about ourselves. Friends know where we work, people talk about us when we are not there
  - People can follow us/track us on social media and physically
- Critics of privacy argue that it gives cover to deception, hypocrisy and wrong doing.
  - Allows fraud and protects the guilty(?)
  - Concern for privacy may be regarded as suspicious – What do you have to hide?
- The desire to keep things private does not imply we are doing anything wrong?
  - On social media, are your accounts private?
  - We may want to keep our health, relationship and family issues private
  - We may choose not to share religious beliefs - to avoid distracting arguments
- Privacy of information can be important to safety and privacy
  - Travel plans, financial data, home address – think of what happens if these are publicly available on social media

Privacy threats

Threats to privacy come in several categories:

- Intentional, institutional use of personal information
  - In the government sector for law enforcement and tax collection
  - In the private sector for marketing and decision making
- Unauthorized use or release by insiders – the people who maintain the information
- Theft of information
- Unintentional leakage of information through negligence or carelessness
- Our own actions (intentional and unintentional)

New technology, new risks

- Government and private databases
  - Bankruptcy records, DNA databases, social media posts, purchase, search
- Sophisticated tools for surveillance and data analysis

  GPS and cameras on mobile devices, internet of things (IOT)
- Vulnerability of data
  - Patient data available online – possibility of breach

New technology, new risks - Examples

- Search query data
  - Search engines collect many terabytes of data daily.
  - Data is analyzed to target advertising and develop new services.
  - Who gets to see this data? Why should we care?
- Smartphones
  - Location apps
  - Data sometimes stored and sent without user's knowledge
  - Companies use the data to build location-based services that are valuable to public/companies
- Why does it matter?
  - Data is vulnerable to loss, hacking and misuse
  - This can pose security issues

Privacy risks

- Anything we do online can be recorded and traced back to our computer/phone/IOTs
- Increase/affordability in cloud storage -> companies/government storing huge amounts of customers'/citizens' data
- People are not usually aware of information collected about them
  - Who reads terms of use?
- Complex nature of software -> businesses don't know what data software's collect
- Leaks happen
- Collection of several small items of information give a detailed description of a person or their life

Privacy risks

- Information on social media is available to everyone; anyone can find it if they look hard enough
- Once information goes online, difficult to delete it
- Very likely that data collected for one purpose (e.g. connecting with friends) will be used for other purposes (e.g. marketing, tracking)
- Government sometimes requests/demands for personal information held by companies
- We sometimes can’t protect information about ourselves; we depend on companies that manage it to protect it
  - From thieves, accidental loss, leaks and governments

Terminology for managing personal data

Informed consent and invisible information gathering.

- Informed consent. Informing people about data collection and use policies so they can decide whether to use a service/tool/app/business or not
- Invisible information gathering. Collection of personal information without a person's knowledge
  - Many companies have policy statements, privacy statements, terms of service/use that inform clients of their policy on collecting and using personal data. Many people don't read them or forget after they do

Terminology for managing personal data

Secondary use. Use of personal information outside the use it was provided for

- Sale of social media information to marketers or other businesses
- Use of text message/social media post for employment decision
- People should have control over secondary use of their information
  - Option to opt in/opt out of secondary use
  - Opt out. People are already in when they sign up for a service (Facebook/Instagram). They have to take action to opt out
  - Opt in. Intentionally sign up for a service

Fair information principles

- Fair Information Principles or Fair Information Practices
  - Principles for protecting personal data
  - Reasonable ethical guidelines
- Inform people when you collect their information, what you collect and how it is used
- Collect only needed data
- Offer an opt out option
- Keep data only as long as is needed
- Keep data accurate; provide means of people to verify and correct their data
- Secure people’s data from theft, accidental leaks
- Create policies for responding to law enforcement requests for data

- Have you used the opt out option of Facebook/Instagram?
- Have you read any privacy policies? Were any deceptive/surprising?

Privacy in social networks

Two aspects of social networks to consider:

- What *we* do - our responsibilities
  - We often want access to information about others but don't want others to have access to same information about us.
    - For e.g. LinkedIn, we want to know who checked our profile but don't want others to know we checked their profile
  - Recruiters can search our profiles for our posts including opinions, religious views, political views during hiring process. What will they find? Is it ethical?
  - People post locations when away on a trip – security issues
  - People care about privacy but don't always act that way on social media

Privacy in social networks

- What *they* do - responsibilities of social network companies
  - Companies deploy new features very often that could affect existing privacy settings
  - New features and selection of default settings
  - Should a social network company introduce new, significant features turned on for everyone? Or should they let people opt in if they want/like the feature
  - Which would you recommend, an opt out or opt in policy?

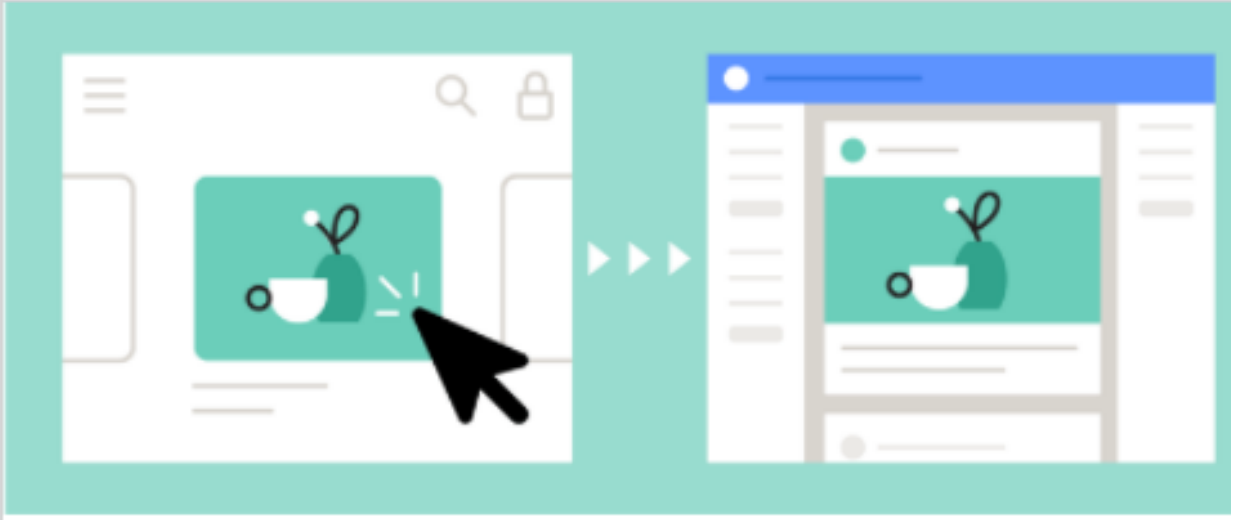
A right to be forgotten

- The right to remove information about themselves from a company's records – e.g. from social media
  - An offensive comment (posted in anger)
  - An offensive comment posted by others
  - A photo
  - News article
  - Personal data posted by others
- Easier when the information is in a person's account
- Should a company always comply?
- How easy is it do delete something from the internet?

Personalized ads in Facebook

Data about your activity from partners

Personalised ads based on your activity on other websites, apps or offline



To show you relevant ads, we use data that advertisers and other partners provide to us about your activity on their websites and apps, as well as certain offline interactions, such as purchases. For example, we may show you an ad for a shirt based on your visit to a clothing website. We never sell your data. Learn more

Choose where we can use data from our partners to show you personalised ads.

Information from partners.

Advertisers, app developers and publishers can send us information through Facebook Business tools that they use, including our social plugins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about your activities off Facebook – including information about your device, websites you visit, purchases you make, the ads you see and how you use their services – whether or not you have a Facebook account or are logged in to Facebook. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its shop. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.

Partners receive your data when you visit or use their services, or through third parties that they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing us with any data. Learn more about the types of partners we receive data from.

Facebook’s use policy

- https://www.facebook.com/policy.php?ref=pf

Avenues for dealing with privacy

- Law
  - Legislation to deal with users/consumers' privacy
- Industry norms
  - Code of conduct that companies have to follow
- Reliance on marketplace
  - Companies in a marketplace can compel operators to abide by privacy principles
- Consumers
  - People should learn to safeguard their privacy
    - Post content responsibly
    - Opt out of services where privacy is an issue
    - Be aware of terms of use

Privacy legislation in Canada

The Canadian Privacy Act.

- Privacy rights regarding interactions with the federal government
- Applies to how government collects, uses, discloses, retains and disposes of personal information.
- Right to access personal information held by government

Collection	Government institution can only collect personal information if it directly relates to its operations
Use	Only for the purpose it is collected for – unless one consents to other uses
Accuracy	Take reasonable steps to ensure information is accurate, up to date and complete
Retention	Retained for at least 2 years unless one consents to its disposal
Disclosure	Can’t be disclosed without consent except in some special circumstances
Access to personal information	One may have access to personal information about themselves

Privacy legislation in Canada

The Personal Information Protection and Electronic Documents Act (PIPEDA)

- Applies to private sector organizations that collect, use or disclose personal information during commercial activity
- Companies must follow 10 fair information principles to protect personal information
  - Accountability
  - Identifying purposes
  - Consent
  - Limiting collection
  - Limiting use, disclosure and retention
  - Accuracy
  - Safeguards
  - Openness
  - Individual access
  - Challenging compliance

Privacy legislation in Canada

- Provincial privacy laws
  - Health related – ON, NB, NF, NS
  - Employment related – AB, BC
- Sector specific privacy laws
  - Bank Act
  - Provincial laws governing credit unions
  - Consumer credit reporting

Privacy legislation in the European Union (EU)

- EU has a comprehensive General Data Protection Regulation (GDPR)
  - Came into law on May 25, 2018
  - Stricter than regulations in US and Canada
- Harmonizes national data privacy laws throughout the EU
- Applies to all companies handling personal data of EU residents
  - Includes companies outside the EU offering goods and services to EU residents
- Covers processing of personal data, collection, use, storage, retrieval, transmission, destruction, etc.
- Processing of data is only permitted if the person has consented unambiguously or if processing is necessary to fulfil contractual/legal obligations
- Prohibits transfer of personal information to countries outside the EU that do not have an adequate system of privacy protection.
- Penalties for non-compliance – fines up to 4% of global annual turnover or €20 million

Privacy legislation in the US

- No standard federal privacy laws
- Has a mix of laws that cover privacy in various sectors
  - HIPPA - Health insurance portability and accountability act (HIPAA) to protect privacy of medical records
  - FCRA – Fair credit reporting act to regulate how credit bureaus disclose financial information
  - ECPA – Electronic Communications Privacy Act restricts the government's use of wiretaps on telephone calls and electronic signals.
  - FTC – Empowers the Federal Trade Commission to go after apps or websites that violates their own (the app or website's) privacy policy
- Some states have comprehensive data privacy laws
  - California – CPRA. California privacy rights act
  - Virginia – VCDPA. Virginia's consumer data protection act
  - Colorado – ColoPA. Colorado privacy act

Reference

- *A Gift of Fire. Social, Legal and Ethical Issues for Computing Technology*. Fifth Edition. Sara Baase and Timothy M. Hemry. Pearson