Cost of privacy

* Scale: focus on individual as opposed to groups/nations (kind of stated in question)
* Quantifying the cost of data in monetary terms. To quantify for a few stakeholders involved - individuals, companies, nations. E.g in case of a data breach, in case of a takeover of a data-centred company

Privacy (big topic)

* Econs
  + Transferable (data can be easily transferred)
  + Inelastic supply (there is only 1; once you sell it, it is gone)
  + Unique price (people value data differently)
  + Reverse economy: Producers (individuals) >> consumers (organisations)
  + Hard to generalize into a market model (cannot use demand and supply - which are aggregations of many producers and many consumers)
  + Market failure
    - Positive and negative externalities e.g. giving data about yourself can affect the people around you as well. There can also be many benefits to society if used properly.
    - Public good e.g. terrorists, suicidal (save lives → justified, no need to pay for data)
    - Imperfect information (individuals do not know the importance / significance of their data)
* Types of data (3 categories) → focus on personal data currently
  + Personal data (ranges from trivial data e.g. name to important data e.g. health, finances)
  + Commercial data e.g. clicks on Facebook
  + Inferred data - ie value added data from companies which analyze your data
* Centralised information framework / data centre for people to sell/buy data [ASSUMPTION] → Who is right for this job? (justification, possible conflict of interest)
  + Security (if we don’t sell the data, people can’t get it) [ASSUMPTION]
  + Ensure that companies cannot sell data amongst themselves (piracy)
    - Similar to music piracy but harder to enforce
    - Government regulatory body
    - Enforce toll on information transfer instead of banning entities (hard to enforce a strict ban) → assign a tag to each individual’s data which will pay a certain “commission” to the individual whenever the data is accessed/transferred
    - Anonymise trivial distribution

Solution for sensitive personal info (referenced from video sent by Hui Kang)

* Store data in a profile database where everything is encrypted → companies can use the data to train the models but they cannot view/access the data itself
* Two possible approaches on how to compensate individuals for data use
  + Pay per use / Subscription (time-based) → focus on this
  + Full control / rights (ie store the data in centralized data companies/data managers) “Super-apps?”,
* Regulate the selling of sensitive information, such as calls and tracking information.

Regulating spread on information on platforms such as social media, info banks (people just share their info on social media, and social media also depend on these info) → use an account database through the centralised info centre i.e. to register for an account on Facebook, you need to establish an account with the centralised data centre first and use that account to sign into Facebook and all data transfer will be monitored and the individual will be compensated accordingly

PI (private information) vs PP (personal property) vs IP (intellectual property)

* NOT THE SAME
* PP and IP, if stolen, do not cause physical harm on the person
* PI, on the other hand, is dangerous when stolen (can potentially harm you)
* Economics differences - material costs, intangible costs.

Saboteurs → people who purposely give fake info / fake personas e.g. creating multiple Facebook accounts

* Legal documentations, verification
* Testing / sensitivity

Super apps (companies that have a lot of your info and can do whatever they want with it) e.g. WeChat

Value to producer (individuals) vs value to consumer

Focus Areas

1. How to charge? (for different kinds of info)

* Perceived cost
  + Come up with an equation e.g. exponential, b\*e^(a\*d-c), where each variable is ranked on a scale of 1-5

1. Importance/Wealth of person
2. Type of data
3. Who we are selling to e.g. economics reason (don’t charge hospitals, etc.), security reasons (terrorists, etc.)
4. Importance of privacy to the individual

* Cannot let the individual decide the price
* Justify subjective ranking and parameters
* RISK

1. Different categories (different values to different people / users)
2. Charge who?

Big data → unstoppable

Time domain - development over time. From the past, to the future developments

Weaknesses? Strengths? Sensitivity analysis?

* **How should data/privacy be priced?**
  + risk/loss function
  + Fairness
    - Risk involved to individual and community
    - Usefulness of data e.g. for profits → remunerate accordingly
  + Utility
    - Social good e.g. communal welfare / altruism (non-economic / non-monetary benefits)
* Threats:
  + Reaping in big profits at the expense of peoples’ safety
  + People don’t know the true value of their data
* **Should there even be a price on safety?** (questioning assumptions) → ethics
  + Most people (e.g. data brokers) do not have bad intentions e.g. doxing
  + We should not put a price on safety, but since we cannot stop people from freely publicising their data, we should put a price on safety to mitigate such actions
* Why are people indifferent about publicising their data?
  + Think that it is inevitable
  + Think that it is convenient
  + Think that people will not have bad intentions
* Right of users to access and download/store their own data?
  + Fairness
  + Prevent large corporations from monopolizing all the data
* **When can this pricing model be used?**
  + Impossible to stop transactions between companies (data can be transferred extremely easily e.g. via thumb drive) → motivation for companies to follow our pricing model (use cases)
  + Evaluating a company / shareholders [REFERENCE]
  + Analyse benefits of data to companies → individuals know how much to sell their information for [REFERENCE, REMEDY]
  + Data breach / hacking cases (fine breached companies, compensation to compromised individuals) [REMEDY]
  + Economic policies e.g. Data Taxation Policy [REGULATION]
* Cycles
  + Rise in prices (data is priced more → companies sell for more?)
  + crypto-data framework
    - Assumes a centralized data framework (all the data is stored in a single place) → not true e.g. each mobile app stores their own set of data
    - Solution: if users can download and store their own data, it becomes a centralized data framework
    - Similar to WeChat, but WeChat is not encrypted
    - Thoughts on Super Apps (WeChat) → we cannot regulate it
* Math
  + **Net Worth** e.g. fraction (risk to individual and community)
    - Risk to community (risk of getting hacked)
      * Defining community worth → status (number of contacts/friends/relationships)
      * Defining individual worth → seniority?? (ranked 1-5) e.g. finance brokers
      * Importance of income/wealth?? → not stated in question, not taken into account in certain scenarios e.g. rich man not interested in cars vs poor man very interested in cars (car dealer)
      * **Possible model: c\*e^(a/d+b+f), where g = net worth, b = seniority, f = type of information, d = constant (chance of getting hacked / losing money), c = profitability / discount factor**
        + Modelled against desired value
        + 2 separate models (with and without externalities)
        + Grounding the model (using data found)

Show that it matches without the externalities

Explain why you include those things this way

* + - How much would you pay to not let your data be released? → more relevant
    - How much would you pay to reverse the data breach? → more relevant
    - How much would a company pay to access your data? → data can be found online; very economic, not idealistic → rephrased: how much should a company pay to access your data?
    - How much remuneration should you get if your data is breached?
  + **Network**