ONE

* + What: From a **big companies perspective, there isn’t really any good reason to not collect data.** Most user data is directly useful to the company in some way or another, and even if it isn’t, the existence of a $200 billion dollar data-broker industry reveals there is a lucrative market for selling on that data.
  + Companies generally believe the **data should be collected in any possible legal ways.** This can include collection directly from the user themselves, or by purchasing from third parties such as data-brokers.
  + The **issue with direct collection from users is that this is often done deceptively.** It is quite commonplace for companies to include clauses in the terms of service that allow data collection from the users that they wouldn’t knowingly agree to. Companies exploit other such similar loopholes, and **whilst they might be legal, we’ve all come to learn that legal does not necessarily mean ethical, and being deceptive surely is not.**
  + The buying and selling to data brokers is also questionable. I don’t think it’s unreasonable to assume most people who share their data with one company, expect they are sharing it with just that one company. With data brokerages however, the data becomes aggregated and shared around to anyone willing to pay for it, possibly for nefarious purposes. This could either be a clear ethical oversight, and thus negligent, or what’s more likely is that it’s fully understood but an accepted consequence, which is just morally reckless.

TWO

* From a companies perspective, the data **should be used because it can provide mutual benefits to the company and its customers.**
  + For example, **the data reveals what the customers like, both at a general but more importantly personalized level.** This allows the company to tailor the product, which improves the product and generates more profit. A potential **downside of such personalization, however, is users being stuck in a positive feedback loop,** in which their views, no matter what they are, are constantly reinforced, which is commonly **referred to as an echo chamber.** These **can be particularly harmful when it comes to politics and issues that naturally divide society, because they further this divide.**
  + Another benefit of data collection is that **ads can be highly targeted and become much more effective, allowing the product to be supported by selling ad space rather than user payments.** The **issue with targeted ads is that it allows companies to unfairly exclude certain audiences.** For example, in 2016, ProPublica bought a Facebook ad for real estate that wouldn’t show to users correlated with African Americans, Asian Americans, Hispanics, and those interested in wheel-chair ramps.
  + **Companies can also argue storing a large amount of data about users increases their security.** How many times have you received **suspicious sign-in attempt** emails and unexpected **2FA** messages? These measures are only possible because companies store data points like **device type, browser, location data, ip addresses, phone-number** and so on. **Without these measures, your account would be compromised.** This is a **double-edged sword** however because just as this information is very effective in protecting you, it is also **just as effective at exploiting you if it is obtained, which is becoming more and more common with data breaches.**

THREE

* + **Companies are for storing the data securely.** It is quite clear that the aforementioned **data breaches incur financial and** **reputational costs** to companies and so **it is in their interest to securely store the data**. **The issue here is that they’re doing the right thing, but not for the right reason.** For an action to be ethical, it must come from a good will, but because the companies intentions are rooted in financial considerations and not moral considerations pertaining to those who the data is about, it’s not too hard to see that they are acting mainly out of self-interest.
  + This is more apparent when answering the question: who has access to the data? Before doing so, It is **also worth noting that user authorization is almost always involved in these situations**, which **implies the company has a duty to protect that user data**.  Companies obviously **believe they have the right to give the data to third parties such as advertisement agencies or to sell it off to data-brokers**, but this begs the question: what is the point of protecting the data with credentials if you simultaneously distribute it? The point is profit, and by favoring profit, they’ve **effectively being morally reckless and ignoring their ethical duty to protect the data.**