“Do tech companies have an ethical obligation to safeguard consumer privacy?”

The question up for discussion is, “Do tech companies have an ethical obligation to safeguard consumer privacy?” But to fully answer this question, a few things need to be addressed, such as

“What is being referred to by ‘consumer privacy’?”

“Who or what does consumer privacy need safeguarding from?”

“What does it mean for something to be ethical?”

To answer the first question, consumer privacy generally refers to their data, such as name, age, email, or even interests/hobbies but it can also refer to generally more confidential things such as credit card info, social security number, address, or passwords.

Who or what does consumer privacy need safeguarding from?

We already know from previous classes that user data is often sold to other companies for advertising purposes, and for many tech companies this IS how they make their money and how they can afford to be free. Since this was discussed before, I will try not to rehash this discussion.

Another entity consumer privacy might need safeguarding from is the government and law enforcement, but that's more of a discussion for a different time.

Right now, I want to focus a third category that consumer privacy needs safeguarding from; criminals, hackers, scammers, and those of a similar ilk. Data breaches of sensitive consumer info that companies are supposed to safeguard can have disastrous consequences for those who get their data leaked.

Some Notable Data Breaches

Home Depot: In 2014 Home Depot was involved in one of the largest data breaches to date involving a point-of-sale (POS) system, leading to a number of fines and settlements being paid. Stolen credentials from a third party enabled attackers to enter Home Depot's network, elevate privileges, and eventually compromise the POS system. More than 50 million credit card numbers and 53 million email addresses were stolen over a five-month period between April and September 2014.

Source: https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

Some Notable Data Breaches

Instagram: In September 2022, Ireland's Data Protection Commissioner (DPC) fined Instagram for violating children's privacy under the terms of the GDPR. The long-running complaint concerned data belonging to minors, particularly phone numbers and email addresses, which was made more public when some young users upgraded their profiles to business accounts to access analytics tools such as profile visits.

Source: https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

Some Notable Data Breaches

Uber: In 2016 ride-hailing app Uber had 600,000 driver and 57 million user accounts breached. Instead of reporting the incident, the company paid the perpetrator $100,000 to keep the hack under wraps. Those actions, however, cost the company dearly. The company was fined $148 million in 2018 — the biggest data-breach fine in history at the time — for violation of state data breach notification laws.

Source: https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

Financial “Obligations” for Safeguarding Privacy

As can be seen from the previous examples, data breaches can cost a lot of money, whether it comes from paying back the affected consumers, other companies involved, or paying government fines.

Let’s focus quickly on the Uber 2016 data breach. This is an interesting case for a few reasons. One being that despite state data breach notification laws probably being known to them, they still tried to circumvent those laws. But in their attempt to do so, they were fined way more than they paid to try to keep it under wraps. But if the risk for this being exposed was so great, why did Uber even take it when following the state data breach notification laws would’ve mitigated the cost of the fines.

While I can’t say for certain, I believe it has to do with the influence and impact of consumer trust.

Caveat emptor, quia ignorare non debuit quod jus alienum emit

The above phrase is the original latin phrase for the concept we call “Buyer Beware”. Wikipedia interprets the phrase as meaning “the buyer should assure himself that the product is good” and cites this as an example of 'information asymmetry'. Defects in the good or service may be hidden from the buyer, and only known to the seller.

While we don’t buy products from many tech companies in the traditional sense, we can think of paying for those products with our data and ability to view ads, which is why some products won’t let you view if you are using an adblocker or may require you to make a trackable account to even use it at all.

If we think about using such products as buying these services with our data, then consumers should do their due diligence to make sure they are “buying” from companies they trust and as such, being seen as a trustworthy and secure company is financial incentive.

Customers Value Safeguarding Their Privacy

About half of the consumer respondents said they are more likely to trust a company that asks only for information relevant to its products or that limits the amount of personal information requested. These markers apparently signal to consumers that a company is taking a thoughtful approach to data management.

Half of our consumer respondents are also more likely to trust companies that react quickly to hacks and breaches or actively disclose such incidents to the public. These practices have become increasingly important both for companies and consumers as the impact of breaches grows and more regulations govern the timeline for data-breach disclosures.

Source:
https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

Companies Need To Make Money

People on the internet sometimes say that the USPS or libraries lose a lot of money each year without understanding that they are not meant to make money necessarily, but rather provide a service to the people. But tech companies are not like that, tech companies exist to generate profits, the services and products provided are simply a means to an end.

Case in point, MoviePass and rabb.it. These two companies (at least before MoviePass was restructured and reworked) provided fantastic services to their users, speaking from experience. However, both companies were very difficult to monetize at the time and thus ended up dying. Their products were too good to exist because they were not able to meet their financial obligations.

Companies Need To Make Money (Cont.)

For an example on the opposite end of the spectrum, let's take Netflix (and other streaming services). There is a theory that the reason that these streaming and entertainment companies haven't conceded to the the demands of the strikers yet is that doing so would involve releasing their real viewership data and that there is a good chance that they have been inflating their numbers to their shareholders. Whether you believe this is true or not, it does highlight the imbalance in the priorities of tech companies because while the penalty for wage theft might be paying a fine or compensating the employees, lying to shareholders can lead to jail time.

Companies generally need to make money, and tech companies are no exception. But, if trust is something that consumers value, then that means it can be used as a selling point. Competition is supposed to be one of the cornerstones of capitalism and if safeguarding consumer privacy is something we care about, we can vote with our dollar for alternatives that are more secure for consumers, and in doing so maybe push the competitors to do the same.

Don’t Be Evil

Google is one of the biggest and most prolific tech companies in the world. But when Google started out, their motto was “Don’t Be Evil”. According to Paul Buchheit, the creator of Gmail, he "wanted something that, once you put it in there, would be hard to take out", adding that the slogan was "also a bit of a jab at a lot of the other companies, especially our competitors, who at the time, in our opinion, were kind of exploiting the users to some extent".

“In 2009, Chris Hoofnagle, director of University of California, Berkeley Law's information privacy programs, stated that Google's original intention expressed by the "don't be evil" motto was linked to the company's separation of search results from advertising.However, he observed that clearly separating search results from sponsored links is required by law, thus, Google's practice had since become mainstream and was no longer remarkable or good.”

Source: https://en.wikipedia.org/wiki/Don%27t_be_evil

Last points I didn’t finish writing

- Ethics are set by some sort of group or organization
- Tech Companies don’t have consistent ethics code like lawyers or doctors
- Closest thing to ethics guidelines are government and laws but problems with that are
    - Government isn’t always ethical
        - Google lawsuit is nearly literally against the foundation of ethics and against the government (U.S. Customs and Border Protection (CBP))
    - Laws will still try to be circumvented like in the Uber example