Privacy regulations in the digital age

Science, Computer Science

In our fast-moving world ruled by technology, one thing that has not kept up with the digital age is privacy regulation. Under the current lack of major privacy regulations in the United States, many technology companies have been able to exploit their user's personal data–information ranging from political leanings to email addresses–for gains in power. When looking for examples of this, one need not look further than the case of Facebook and Cambridge Analytica.

Cambridge Analytica was a data analytics firm that worked the campaigns of Brexit and Donald Trump to predict and influence choices at election time through targeted Facebook posts and advertisements. Facebook mistakenly allowed them to exploit a feature of the site allowing them to use a personality test meant to be shared with friends for fun to gain access to over 50 million Facebook users' friends, personal information, and posts. The societal implications from a company gaining the ability to personally target voters to sway their opinions without them even knowing it are huge. In an interview with The Observer featured in The Guardian, Christopher Wylie, a whistleblower amongst the people who harvested the data for Cambridge Analytica, explains: " We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on." This admission confirms the intentional manipulation of public opinion allowed by the current lack of proper digital privacy regulation. The fact that the government did not intervene in this until 2018 even though Cambridge Analytica started this process in 2014 is a sign that privacy regulations are due for an update.

Solution

One promising solution to these problems is the GDPR, recently implemented by the European Union. The GDPR (General Data Protection Regulation) defines basic principles that companies must follow when collecting data on their users, which, according to IT Exchange, include transparency of what is being collected to the user and to the government and ensuring the security and confidentiality of the data. If a company does not follow these regulations, then the EU can impose fines upon them.

Both the transparency and security principles of the GDPR would have prevented the Cambridge Analytica firm from being able to provide the service that it did. The EU, through the GDPR, would have taken actions against Facebook to stop this, because Facebook would have, following the transparency principle, made known the volume of data available to the personality test used by Cambridge Analytica, and, once Facebook knew about the breach in data, it would have been punished for the breach in security, and as well Facebook would have been pressured to announce that the breach had happened years before it decided to on its own. The benefits from privacy regulations such as the GDPR extend beyond the narrow focus of Cambridge Analytica. For example, these regulations prevent practices such as selling users' data to marketers for a profit or targeting users' interests in advertisements without letting them know they are being manipulated.

While reasonable and foolproof in principle, digital privacy regulations such as the GDPR still possess a few problems preventing them from making their

way into the United States government anytime soon. For example, while staying transparent about every piece of data collected on a company's users is a great thing, it is cumbersome for businesses to implement– especially small businesses. Requiring additional investment in legal consultation, compliance officers, and paperwork, many small businesses would be harmed by these regulations, and creating an innovative technology startup would be much less profitable, stifling a main motivation for innovation at the source.

Closing

The United States should not rush into mimicking the popular yet not America-compatible GDPR out of desperation. The benefits of having digital privacy regulations such as the GDPR are apparent, but so are the disadvantages. The United States should implement these regulations to avoid incidents such as Cambridge Analytica from ever happening again. However, the United States would be heavily impacted by regulations exactly like the GDPR due to them being harmful to small businesses, and according to the U. S. Small Business Administration, in 2008, a large 46% of the private nonfarm GDP belonged to the very small businesses that would be hurt by these regulations. By implementing these regulations exactly as they are in the EU with no revisions, small businesses, and therefore a large section of the economy, would suffer; therefore, the United States should not implement any data privacy regulations as overarching and burdensome as the GDPR until a serious discussion occurs to plan a way to compromise

between the privacy of the users of technology and the economic viability of small businesses that hold together the fabric of the American economy.