Global Counsel

US data brokers on notice as Congress and regulators sharpen their focus on sector

Blog post by Senior Associate Miranda Lutz, 13 January 2022

Online clicks and webpage visits have been tracked for decades; now data collection has leapt from the screen to the physical world. In 2020, there were more than 11 bn connected Internet of Things (IoT) devices, from appliances to wearable health monitors. That figure is projected to more than double to 27 bn by 2025, according to IoT Analytics. Each one of these devices represents a new vector for consumer data collection.

In the US, there is no federal law or regulatory framework to govern the collection, use, and sale of consumer data whether it is collected via websites or through devices. The explosion of tech-related policy challenges has muddied the waters on legislative efforts to regulate the industry – even when there is bipartisan support. It has become impossible for lawmakers to separate data protection from antitrust/competition, content moderation and cybersecurity, each with its own host of controversial policy debates.

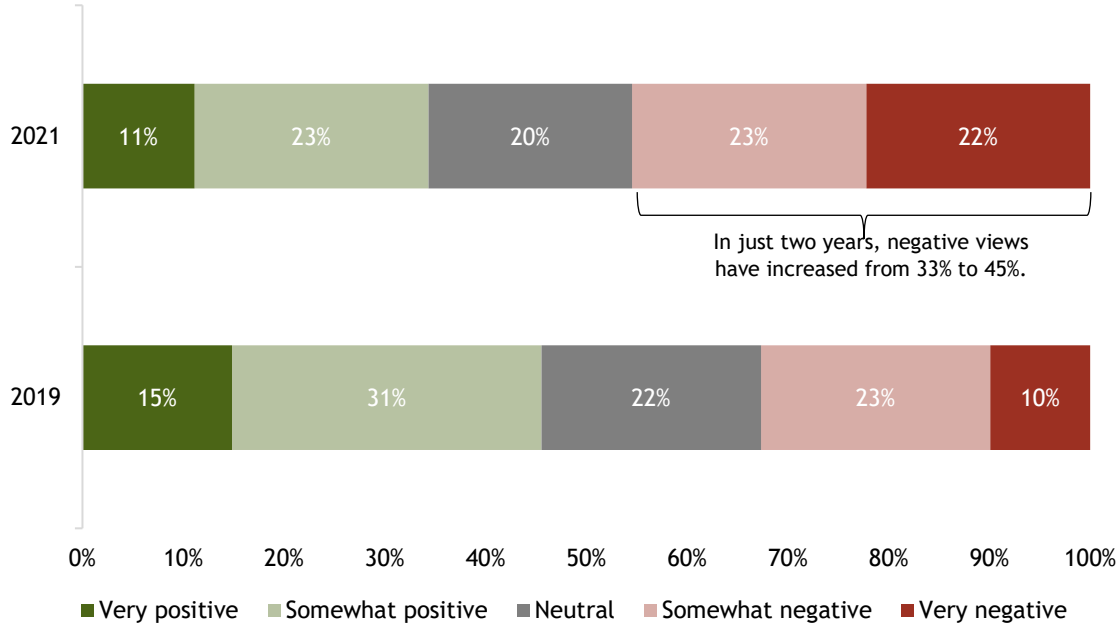
As a result, US states have taken the lead on data privacy laws, but the US has already effectively ceded regulatory control to Europe, the UK, and other jurisdictions, as many US-based tech companies operate internationally. Belatedly, a bipartisan group of lawmakers on the Finance Committee including Senators Bill Cassidy (R-LA) and Ron Wyden (D-OR) have begun to scrutinize third-party data brokers, companies that collect and sell personal data with no direct relationship to the consumer.

Lawmakers identified what they view as particularly problematic practices by data brokers. These include harvesting or selling user health or location data. It also includes to the sale of data regarding US military personnel or government employees, which could pose a national security risk. Conversely, advocates and certain lawmakers have expressed concerns that US law enforcement agencies can access information on suspects via data brokers that would traditionally require a court order.

Despite the slow start, the direction of travel for US policy is toward greater restrictions around the collection, storage, processing and sale of consumer data. The fact that a group of Senators from both sides of the aisle has zeroed in on certain types of data and data brokers suggests targeted legislative action could be forthcoming. This type of tailored approach has been more successful of late in gaining bipartisan support even amid partisan gridlock; for example, the nearly $1tn bipartisan infrastructure package passed in late 2020.

Growing scepticism of Big Tech from consumers and policymakers (see figure below) is driving meaningful changes in the way companies use consumer data in the US. Tech companies are voluntarily making changes to their products, such as shifting away from third-party cookies while browsing the web, for example.

Americans' sentiment towards technology companies



Source: Gallup

The rapid growth of privacy-focused tech products like encrypted email and private search engines are further indicative of the change in sentiment. Governments are also starting to take notice. In December, the US and UK announced a joint initiative announced a collaborative effort to support privacy-enhancing technologies (PETs).

For data brokers, these are important developments. Although wholesale regulation will be slow to develop in the near-term, there are several policy trends that merit attention:

- **The Biden administration's regulatory officials are expected to pursue more enforcement actions against technology firms; key Biden appointees have taken a distinct interest in consumer data protection.** Under Chair Lina Khan, the Federal Trade Commission (FTC) may pursue a sweeping data privacy rulemaking in 2022, although any regulation of this nature would take years to implement. The biggest near-term risk is that the FTC substantially increases its investigations into potential deceptive practices and abuses connected to consumer data. Providing consumers an easy way to opt out of their data collected and sold to third parties could mitigate risks of regulatory scrutiny. But it is important that companies do not discriminate against consumers who decide to opt out. Companies that do not accurately and clearly disclose how they collect, use and sell consumer data will be targeted. The FTC's efforts are likely to be bolstered by increased government spending as Congress is likely to fund a new privacy-focused unit within the FTC. For an agency that has long complained that a lack of resources has held it back from serious enforcement, the funding could be a gamechanger.
- **Under Rohit Chopra, the Consumer Financial Protection Bureau is likely to try to expand its mandate to Big Tech.** In one of his first orders as CFPB director, Chopra (himself a

former FTC Commissioner) instructed Big Tech companies like Amazon, Apple and Facebook to turn over information to the CFPB on how they gather and use consumer payment data. Chopra and the CFPB are especially interested in how these Big Tech companies use harvested data for behavioural targeting that may not align with consumers' expectations. The request for information could lead to greater regulatory restrictions around how consumer financial data is bought and sold – often a critical data resource for third-party data brokers.

- **The Securities and Exchange Commission (SEC) has also shown an interest in alternative data providers.** In 2021, the SEC fined data broker App Annie for violation of the anti-fraud provisions of Section 10(b) of the Exchange Act, which prohibits deceptive conduct and material misrepresentations in connection with the purchase or sale of securities. In its investigation, the SEC alleged that App Annie "lied to companies about how their confidential data was being used." Investigating alternative data providers also appeared on the SEC's most recent Examination Priorities. Web scraped data that is sold to investors should expect to come under greater scrutiny, especially since such data is not available to the average investor. Companies in the web scraping business should be prepared to demonstrate how they prevent the collection of material non-public information. Furthermore, firms working with third-party data brokers should ensure they conduct regular due diligence or trusted supplier network for their vendors to ensure that vendors are ethical and responsible stewards of consumer data. Companies may want to consider whether it is more sustainable in the long run to bundle web scraped alternative data into broader industry or sectoral trend data to avoid the risk that may come from selling data related to the performance of publicly traded companies.

These developments – combined with evolving consumer preferences and further growth in IoT – are likely to change the regulatory landscape for third-party data brokers over the next several years. First-party data collections and third-party data brokers should begin to consider how they could implement a *modus operandi* of data minimalisation instead of data maximization. The era of unregulated data collection is over. It is just a matter of time.