CRS INSIGHT

Data, Social Media, and Users: Can We All Get Along?

April 4, 2018 (IN10879)

|

Related Author

- Chris Jaikaran

|

Chris Jaikaran, Analyst in Cybersecurity Policy (cjaikaran@crs.loc.gov, 7-0750)

Introduction

In March 2018, media reported that voter-profiling company Cambridge Analytica had exceeded Facebook's data use policies by collecting data on millions of Facebook users. Cambridge Analytica did this by working with a researcher to gain access to the data, so the company itself was not the entity seeking access to the information. This allowed Cambridge Analytica to "scrape" or download data from users who had granted access to their profiles, as well as those users' Facebook friends (whose profiles the first user had access to, but for which the friends did not authorize access).

At this time, it is publicly unknown what data were accessed. Facebook hired a digital forensics firm to audit the event. Based on media reporting and old Facebook applications, user profile data such as interests, relationships, photos, "likes," and political affiliation may have been accessible, but not all data held by Facebook appear to have been accessed by an outside party. Additionally, as initial access to a user's profile was granted via an app, other information about the user, such as other apps installed on the device and Internet Protocol addresses, may have been accessed. With this information, Cambridge Analytica built profiles of potential voters to test messaging and target advertisements. In addition to ads on Facebook, search engine optimization may have been used to drive users toward ads and other web content (i.e., blogs) outside Facebook.

This event could be characterized as a data breach despite Facebook systems not being

breached (i.e., hacked) because a third party was able to access data that neither users nor Facebook intended to share. Rather than compromise a vulnerability in Facebook's information technology (IT), Cambridge Analytica compromised weak security controls and violated Facebook's data policies. This breach is akin to an insider exceeding authorized access to retrieve information, or an outsider using information they were authorized to access for purposes prohibited by contractual agreement.

In response to this incident, some Members of Congress have questioned Facebook and have invited Facebook CEO Mark Zuckerburg to testify before House and Senate committees. This Insight examines policy issues surrounding this incident and provides options for Congress to consider. While this event has started discussions on election security and social media company requirements to report advertising, this Insight addresses data security concerns without discussing the impacts or consequences of data use.

Issues

This is not Facebook's first major privacy and data security incident. In 2011, the Federal Trade Commission (FTC) entered into a consent order with Facebook following an investigation into the company's privacy practices at the time. The FTC went further and released guidance so other companies could avoid enforcement actions. In an unusual step, the FTC has publicly confirmed opening an investigation on Facebook's data security and privacy practices in light of the media reports about Cambridge Analytica.

While Facebook's, the FTC's, Congress's, and other investigations continue, the public will learn more about this event and its implications. However, initially, this event has ignited a public debate on data ownership, usage, security, and privacy.

Data Ownership, Rights, and Usage

Consumers' expectations and reality on who owns data and how data may be used are commonly misaligned. In Europe and Canada, data about individuals are generally considered to always remain their data; they have a right to the data, a right to expect the data be secured, a right to know exactly how those data are used, and a right to remove those data from the service hosting it. However, in the United States, general data regulation does not exist. Individual regulations exist, but those are targeted at specific types of entities (e.g., the Safeguard Rule for financial firms and HIPAA health information standards for payers and providers of healthcare). Once data are submitted to another entity, they are generally considered to be under that entity's ownership, and any data that entity generates from submitted data belongs to that entity—barring a separate agreement between the parties dictating data ownership and usage.

Data Security and Privacy

Data security is not generally prescribed by law for the information technology sector. Instead, companies make IT security investments as part of managing corporate risk. Mitigating this risk may be material to their investors or beneficial to their users. In the U.S. system, privacy rules are in place to ensure privacy of an individual from the government. However, privacy of individuals from other entities (e.g., other individuals or corporations) is a matter of state law

and private agreements (e.g., contracts). This places a higher burden on individuals to understand the risk of generating and sharing data, as well as reviewing and understanding individual agreements with different services with which they engage.

Options for Congress

Oversight

Congress has provided oversight of data security practices at private companies in the past. Following the Equifax data breach last year, Congress held hearings on the incident and encouraged the industry to adopt stronger security postures and provide consumers relief. Hearings can inform legislation, advance debate, and drive private action in hopes of avoiding governmental action.

Legislation

Options for Congress to legislate in response to the Facebook incident include (but are not limited to) defining national expectations for data ownership and privacy establishing expectations for liability when unauthorized parties access data; and creating data breach notification rules. Examples of such rules are the European Union's General Data Protection Regulation (GDPR) and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

These options would alter companies' relationship with data. Currently, data are cheaply collected, analyzed, and used for profit, enabling free access to large portions of the Internet and other IT services. Placing restrictions on data would alter the business models of these Internet-enabled companies and services. The question then becomes one of tradeoffs—does the free use of data create a national harm or is it a necessity for America remaining a leader in innovation, and what are the consequences of each?

In considering legislative options, Congress could also consider granting regulatory authority to a federal agency or agencies, or it could create a new federal entity to regulate companies. It appears that agencies do not currently have authority to regulate the data security at social media companies. Instead, data security may be enforced at a company pursuant to a consent order with the FTC after an unfair or deceptive practice investigation.

Regulation

The IT sector (including social media companies) currently faces little federal regulation. This stems from a desire to promote innovation. However, absent from that argument is the enormous social and economic impact of some IT companies. For instance, the reported 50 million Facebook users affected by this event is greater than the estimated populations of New York and Texas combined, and Facebook has a larger market capitalization (over $400 billion) than JP Morgan Chase (over $300 billion).

Congress could consider several models for regulation, including

- **Government Regulation**—a government agency directly regulates an industry through an exercise of statutory authority with accountability to the President and Congress

(e.g., the Nuclear Regulatory Commission's relationship with nuclear facilities).

- **Quasi-Governmental Regulation**—an organization with public and private sector characteristics, like a government corporation, regulates under a statutory authority and has accountability to the President and Congress (e.g., the Federal Deposit Insurance Corporation).
- **Regulation by Nongovernmental Elements**—a nongovernmental entity exercises regulatory authority in cooperation with, or under the oversight of, a governmental agency (e.g., the North American Electric Reliability Corporation writes standards which are accepted and enforced by the Federal Energy Regulatory Commission).
- **Self-Regulatory Organizations (SROs)**—organizations that act under a federal statute or authority, which can be overseen by a government agency (e.g., the Financial Industry Regulatory Authority) and federally chartered organizations that have exclusive jurisdiction over a specific subject (e.g., the U.S. Olympic Committee governing U.S. participation in the Olympic games).

If Congress were to grant regulatory authority to a federal agency or agencies, agency action would probably fit into a three-step framework. First, an authorized entity *creates* the regulation which industry must follow. This is also called *rulemaking*. Next, an agency could *examine* or *supervise* for compliance with the regulation. If a company is found to be not in compliance with the regulation, the agency could *enforce* the regulation (e.g., suing the company or issuing a fine). Congress may grant authority to different agencies for each step in this framework.

Should Congress legislate and/or grant regulatory authority to a new or existing entity, Congress may likely have an interest in conducting oversight of how that authority is executed.

Another option, which does not require congressional action, is for industry-based SROs to prescribe standards (e.g., the Payment Card Industry Data Security Standards). In such instances, the government does not compel participation in the scheme, though industry-specific factors might make nonparticipation difficult.