The National Security Imperative of Protecting User Data

Carrie Cordero

Carrie Cordero is the Robert M. Gates Senior Fellow at CNAS.

SUMMARY

The current policy debate surrounding potential regulation of technology companies and how they handle data focuses exclusively on the privacy of that data. The debate is framed as a debate over privacy legislation. This brief argues that the policy debate about how technology companies collect, retain, handle, share, and sell user data and provide access to users should be broader than privacy considerations; it should also take into account the national security implications of protecting data collected by the private sector. In other words, privacy legislation directed at 21st-century technology platforms and internet companies is not just about privacy; it is also important to address modern-day national security threats.

KEY ISSUES

Incorporate national security considerations into the debate over technology platform collection and use of personal data.

Refine privacy legislation proposals to focus on enterprise-wide privacy protections that place the burdens of protecting user data and use on companies hosting technology platforms, not individual users.

Ensure that congressional intelligence committees can continue to monitor foreign influence efforts directed at U.S. democratic institutions through reporting requirements.

DATA PROTECTION IS NOT JUST A PRIVACY ISSUE, IT IS ALSO A NATIONAL SECURITY ISSUE

Policy debates over national security legal authorities, like surveillance, have traditionally pitted those favoring national security equities against those favoring privacy equities. The choice is a false one. Particularly in light of what has been revealed about the intelligence activities conducted by the Russian government to interfere in the 2016 election, corporate data collection and private sector data user policies are more than a privacy issue, they are also a national security issue.[1]

What is evident from the investigations and reviews of Russia's 2016 and ongoing election interference activities, is that the security of data retained by social media companies, the access to the platforms by third parties, and the transparency provided to users, all require a legal framework. As part of its ongoing comprehensive investigation into Russian election interference in 2016, the Senate Select Committee on Intelligence (SSCI) commissioned independent third parties to conduct analyses of how the Internet Research Agency (IRA) exploited U.S. social media platforms. One of the two reports, entitled *The IRA, Social Media and Political Polarization in the United States, 2012–2018* (the Oxford-Graphika Report), investigated "how the IRA exploited the tools and platforms of Facebook, Instagram, Twitter and YouTube to impact U.S. users." The Oxford-Graphika Report identified IRA activity on social media platforms as far back as 2012, and includes substantial analysis revealing that the IRA use of social media platforms "demonstrates a sustained effort to manipulate the U.S. public and undermine democracy."[2] The second report, entitled *The Tactics & Tropes of the Internet Research Agency* (the New Knowledge Report), reviewed social media posts and metadata provided to the SSCI by several Internet platforms, and found that the IRA created a "manipulation ecosystem."[3]

1. Carrie Cordero, "Corporate Data Collection and U.S. National Security: Expanding the Conversation in an Era of Nation State Cyber Aggression," Lawfare, June 1, 2018, https://www.lawfareblog.com/corporate-data-collection-and-us-national-security-expanding-conversation-era-nation-state-cyber. (As outlined in this address at Georgetown Law's Cybersecurity Law Institute in May 2018, private sector data collection poses unique challenges because it: (i) collects directly from individual users; (ii) is not subject to consistent or mandatory standards for handling; (iii) data can be moved around without the user necessarily being informed; and (iv) data is for sale.)

2. Philip N. Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly and Camille Francois, Computational Propaganda Research Project, "The IRA, Social Media and Political Polarization in the United States, 2012-2018" (Oxford-Graphika Report), (University of Oxford, 2018), 39, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf.

3. Renee DiResta, Dr. Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Dr. Jonathan Albright and Ben Johnson,

CNAS

"What is evident from the investigations and reviews of Russia's 2016 election interference activities, is that the security of data retained by social media companies, the access to the platforms by third parties, and the transparency provided to users, all require a legal framework."

The Oxford-Graphika report further explained that there was significant disparity between how companies cooperated with the SSCI-commissioned review.[4] The companies provided only a "snapshot" of data to investigators in the summer of 2017.[5] The companies provided different categories of information and provided it in different formats.[6] Some companies provided extensive data, others provided a moderate level of cooperation, and some companies did not appear to provide data in a way that could be analyzed by the third-party analysts. Given the continuing nature of the threat, if companies are not going to voluntarily comply, then Congress should institute reporting requirements so that the government can conduct ongoing analysis of how the threat is evolving. In other words, the reviews commissioned by the SSCI for the current investigation should not be isolated reviews. Instead, the intelligence committees should take on continuing responsibility to monitor this particular activity, which is at the intersection of industry and national security. To do that, the companies will need to cooperate with Congress's work in a more regularized manner, and more consistently across the industry.

Companies cannot be expected to self-regulate to a sufficient degree that protects Americans from a hostile nation-state intelligence activity.[7] With respect to the activities that took place leading up to 2016, the companies were not in a position to understand the severity of the threat, and, once identified, were not able or willing to move quickly and expansively enough to neutralize the activities taking place on their platforms. While technology companies have taken steps to make their users' privacy more protected and their platforms more secure, each company has taken different steps and the activities are voluntary. As a result, even leaders in the industry recognize that government regulation is needed.[8] Companies cannot be expected to do government's job for it.

A regulatory environment directed at the internet technology industry generally and social media companies more specifically must consider not only what data the companies collect and retain and how they use, share, or sell it, but how outside actors can reach a company's user base. As Pierre Omidyar, Ebay's founder has stated, "the monetization and manipulation of data is swiftly tearing us apart."[9] The mere existence of social media platforms and society's use of them has provided a vector through which a hostile foreign power can exert influence. With respect to Twitter data, for example, the Oxford-Graphika Report found that the IRA used its false accounts on the platform in way that its influence campaign was "effectively woven into the fabric of online U.S. political conversations right up until their suspension."[10]

"The Tactics & Tropes of the Internet Research Agency," New Knowledge (December 17, 2018), 2, https://www.newknowledge.com/articles/the-disinformation-report/.

4. Oxford-Graphika Report.

5. Oxford-Graphika Report.

6. Oxford-Graphika Report.

7. As noted in the Oxford-Graphika Report, 10, "We clearly observe a belated and uncoordinated response from the platforms that provided the data."

8. Mark Zuckerberg, "The Internet needs new rules: Let's start in these four areas," *The Washington Post*, March 30, 2019, (stating that companies need to be regulated "in four areas: harmful content, election integrity, privacy and data portability"), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?noredirect=on&utm_term=.d50e84dc1c76.

9. Pierre Omidyar, "6 Ways Social Media Has Become a Direct Threat to Democracy," *The Washington Post*, October 9, 2017, https://www.washingtonpost.com/news/theworldpost/wp/2017/10/09/pierre-omidyar-6-ways-social-media-has-become-a-direct-threat-to-democracy/?noredirect=on&utm_term=.96b5a1803233.

10. Oxford-Graphika Report, 27.

Americans do not have enough information about or control over what happens to their digital information. For example, during the 2016 election season, Facebook provided information concerning over 50 million users to Cambridge Analytica, which had been hired by the Trump campaign.[11] While on its face a privacy and compliance issue, the transfer of such volume of information—unbeknownst to the users—to a political entity raises the question of how information can be used in an unauthorized way. The ability of Facebook to easily transfer information to an outside entity raises the issue of whether the same type of information, and high volumes of it, are vulnerable to foreign powers seeking to exploit that information for intelligence or other purposes. And, the episode highlighted the inadequacy of remedies for individuals whose information was transferred. Other than evaluating whether a consent decree had been violated or asking the company to provide information to Congress or testify, there has been an inadequate basis upon which government can hold companies accountable.[12]

"The ability of Facebook to easily transfer information to an outside entity raises the issue of whether the same type of information, and high volumes of it, are vulnerable to foreign powers seeking to exploit that information for intelligence or other purposes."

NEXT STEPS: BROADENING THE LEGISLATIVE DEBATE

The time for comprehensive data protection legislation seems to have arrived. Reasons for the issue gaining traction in the United States include but are not limited to:

- the pervasive compromises and exposures of Americans' data through unauthorized access;
- global concerns about government access to data from private sector entities for law enforcement and national security purposes;
- conflicting laws and requirements in the United States and EU for companies that do business and have substantial user bases on both sides of the Atlantic; and
- greater understanding in United States following the 2016 election regarding how Americans' data held by social media companies can be manipulated by a hostile foreign intelligence service.

Proposals for new U.S. privacy legislation are beginning to focus more on the responsibilities of the private sector entities themselves versus the responsibilities of individuals.[13] While opt-in or opt-out provisions provide some level of privacy protection for the savvy and engaged technology user, these provisions are adequate from neither an enterprise privacy or a national security perspective. From a comprehensive privacy protection perspective, users opt-in by default because they either do not take the time to read the notice provisions, the provisions are too dense to read, or, by virtue of the reason for using the service or technology, the user has, essentially, no choice but to opt-in.[14] Certain apps and technology services have become so much a part of daily American life that the notion of opting out of the service would mean forgoing participation in a work, education, or community activity. Moreover,

11. Kevin Granville, "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens," *The New York Times*, March 19, 2018, https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

12. Kevin Granville, "Facebook and Cambridge Analytica."

13. Cameron F. Kerry, "Breaking Down Proposals for Privacy Legislation: How Do They Regulate?" (Brookings, March 8, 2019), https://www.brookings.edu/research/breaking-down-proposals-for-privacy-legislation-how-do-they-regulate/ ("A change in the paradigm of privacy regulation from consumer choice to business behavior means that law will have to supply these checks.")

14. Editorial Board, "How Silicon Valley Puts the Con in Consent," *The New York Times*, February 2, 2019, https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html.

with respect to the national security considerations present in the mass collection and use of Americans' data that is subject to malign foreign cyber activity, individual user preferences and selections are essentially meaningless.

Congress should take a broader look at private sector data collection and retention beyond just viewing legislative proposals from a privacy perspective. Although policymakers need to be cautious about framing issues as a national security risk for purposes of expedience, the Special Counsel and SSCI investigations of the Russian intelligence operation targeting the 2016 election and western democratic institutions reveal that mass private sector data collection and Internet platform use presents a fundamental risk to the effective functioning of U.S. political systems.[15] Accordingly, a privacy-protection legal framework that more significantly takes into account national security would also include:

» requirements for data security at an enterprise level, consistent with the fluid development of new technologies and security best practices;

» requirements for reports to congressional intelligence committees and public reporting regarding evidence of foreign influence on the platform; and

» requirements for enhanced cooperation with the intelligence community regarding identification of significant foreign efforts to infiltrate the platform or obtain unauthorized access to user personal information on a large scale.

15. Laura K. Donohue, "The Limits of National Security," 48 Am. Crim. L. Rev. 1573-1756 (2011), https://scholarship.law.georgetown.edu/facpub/1010/.