MURRAY STATE UNIVERSITY Commonwealth Review of Political Science

Volume 4 | Number 1 Article 4

2017

A Case Study on American Social Media Privacy: Facebook and Government Oversight

Sarah Fink
Morehead State University

THE COMMONWEALTH REVIEW • Volume 4, Number 1 • 2017

http://www.kpsaweb.org/CRPS

A Case Study on American Social Media Privacy: Facebook and Government Oversight[1]

Sarah Fink
Morehead State University

As we move further into the age of technology, there is no reason to expect the use of social media and the internet will decline. The government's inability to create a uniform technological landscape across offices and departments around the nation along with the shifting view of privacy in America has created openings for non-governmental companies, like Facebook, to collect the information freely given by citizens. This makes the privacy policies of social media companies civil rights and liberties issue for individual citizens as well as a national security concern. This paper argues that until the public, and policy makers, understand the threat of a new body controlling mass amounts of information on the American public, few concrete steps will be taken to protect users' privacy and the integrity of the country's data infrastructure.

Key Words: Facebook, social media, privacy, data security

Today, technology drives everything we do from how we keep up with our schedules to how the entire U.S. government functions. Information that used to be stored in complex filing systems can now be found with the click of a button. While this technological revolution has made many governmental functions quicker, it has opened the door for a new concern regarding citizen privacy. Personal information held by governmental offices was previously hard copy forms stored in locked cabinets, in secure rooms, in guarded offices. While the risk of information theft was still present, it was much more of a feat to break in and steal one hard copy than it is to download thousands of digital files. There remain legal and ethical obligations to protect the privacy rights of

[1] I would like to express my gratitude to Dr. Michael Hail and the Intelligence Community Center of Academic Intelligence at Morehead State University, as without their support and guidance this research would not have been possible. I would also like to thank my parents, Bill and Kaye, and mentor, John, for encouraging me to ask the hard questions.

citizens for government even while there are increased risks.[2] Modern day breaches can lead to the release of mass amounts of personal information ranging from credit card numbers, social security numbers, to home addresses and phone numbers. With the large amount of citizen data stored on government servers, all levels of government have become targets for amateurs looking to make money on the black market and larger, more organized, non-state actors.

Local, state, and the federal government have increased security measures and changed the way in which they work together to protect private information. However, with the inability to create effective policy in the ever-changing world of technology and the lack of technology in smaller rural areas, a divide has been created within the government. This divide does not relate to political views, gender, or other issues of the sort, but to the equipment and technological capabilities of those in government. The lack of a uniform understanding of technology across the states has led to smaller rural areas having less ability to survive in a government run by technology. Local and state governments with less equipment or understanding are at a disadvantage when competing with larger more urban areas. Due to this divide between the under-equipped and the over-advanced, the United States is now facing an information crisis like never before.

Aiding in the struggle of the government to keep up with technology is a public shift in attitude towards privacy. Younger generations are growing up with social media encouraging an open sharing of even the most intimate aspects of human life, while older generations are unaware of what sites to trust and who to give information to. In a Morning Consult/Politico poll from 2017 it is clear the public does not know who to trust when it comes to social media. The issue of privacy is still a bipartisan issue with 56% of registered Democrats and 60% of registered Republicans stating they did not believe the media giant Facebook would keep their data private, numbers sure to have risen since the Zuckerberg scandals in 2018.[3] Those above the age of 18 are entering the years of applying to colleges, looking for employment, and creating a family leading to a more conscious view of what they post on social media. However, without regulation or a uniform understanding of how information is gathered by these social media sites it is easy to predict social

---

[2] Hail, Michael W. "Federalism, Privacy Rights, and Intergovernmental Management of Surveillance: Legal and Policy Issues." Book chapter in: *Video Surveillance*, edited by Weiyao Lin. Rijeka, Croatia: InTech Publishing, 2011, 27-34.

[3] Nasr, Amir. Poll: Little Trust that Tech Giants will Keep Personal Data Private. (10 April 2017). Retrieved from Morning Consult: https://morningconsult.com/2017/04/10/poll-little-trust-tech-giants-will-keep-personal-data-private/

media bypassing the government in an understanding of its citizens and their habits.

The government's inability to create a uniform technological landscape across offices and departments around the nation along with the shifting view of privacy in America has created openings for non-governmental companies, like Facebook, to collect the information freely given by citizens. These openings are secured by the lack of education in the public on what information Facebook collects, how the information is collected, and how the information is shared. Until the public, and policy makers, understand the threat of a new body controlling mass amounts of information on the American public there will be no steps taken to protect user's privacy.

THE FACEBOOK DATA POLICY

To fully understand what is at risk with the information gathered on social media sites, it is important to understand the complex world of privacy and data policies. These policies are designed to outline the usage of any information provided by a user. However, often these policies are complex legal documents confusing the average user. Facebook's Data Policy is no different. The site claims to simplify the privacy process by creating shortcuts, it steers users away from the actual data collected by the site and how this data is used.

Facebook's Data Policy currently contains options for the companies to collect information regarding a user's name, email, location, and habits. From information regarding how often a user checks the site or their notifications addictive tendencies can be deduced. Similarly, the information stored regarding the type of communications with other members and groups along with the duration and frequency of these discussions can lead to information regarding social habits. Facebook also collects data pertaining to how often others post, share, and tag a user determine who the user spends large amounts of time with. These factors along with the information gathered on the user's devices can lead to a large amount of identifying information being stored on a single individual and their network of friends. However, the Facebook site is not the only collector of data in the Facebook empire.

The Facebook Data Policy allows the company and its child companies to collect physical, geospatial, and intellectual content from its users. Users accept this policy when they create an account and join Facebook, however, few know what this policy really contains. The current Data Policy aims to outline the data usage and collection of the site and the controls users have over their information. Users can opt out of sharing information with certain

third-party partners, but cannot control what information is gathered and shared with Facebook and its child companies.[4]

The data collected by the Facebook Companies can be broken down as either identifying or non-identifying information. While these data policies do not specifically state what information is identifying or non-identifying the data can be broken down using the Department of Homeland Security's definition of "identifying data." DHS uses the definition, "any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual" to separate identifying and non-identifying data.[5] Using this definition the data gathered by Facebook and its nine child companies, Facebook Payment, Atlas, Instagram LLC, Onavo, Moves, Oculus, WhatsApp Inc, Masquerade, and Crowd Tangle.

Each of these companies collect different types of data based on their operations. Facebook Payments, Instagram, and WhatsApp Inc. are the most well-known of the Facebook companies, with Facebook Payments being the platform for financial transaction, Instagram being an image based social media platform, and WhatsApp being a messaging application. Facebook Payments is the most secure of the Facebook companies in terms of privacy sharing the bare minimum information required for processing and security.[6] Instagram, much like Facebook gathers both identifying and non-identifying information on its users.[7] WhatsApp collects identifying information pertaining to senders, receivers, and message time and date, but not the message content.[8] The other Facebook companies are less well known. Atlas is an advertising platform which collects large amounts of demographic data on its users.[9] Similarly, Crowd Tangle is an analytics program which gathers information on what demographics view user's advertisements.[10] Onavo helps in lessening the data usage on mobile devices and mainly collects information on the device it is

---

[4] *Data Policy.* (29 September 2016). Retrieved from Facebook: https://www.facebook.com/about/privacy

[5] Handbook for Safeguarding Sensitive Personally Identifiable Information. (2012). *U.S. Department of Homeland Security.*

[6] *Facebook Payments, Inc. Privacy Policy.* (30 December 2013). Retrieved from Facebook: https://www.facebook.com/payments_payments_terms/privacy

[7] *Privacy Policy.* (19 January 2013). Retrieved from Instagram: https://help.instagram.com/155833707900388

[8] *WhatsApp Legal Info.* (25 August 2016). Retrieved from WhatsApp: https://www.whatsapp.com/legal/#privacy-policy

[9] *Privacy Policy.* (13 April 2015). Retrieved from Atlas by Facebook: https://atlassoulutions.com/privacy-policy/

[10] *Privacy Policy.* (11 January 2017). Retrieved from Crowd Tangle: http://www.crowdtangle.com/privacy

operating within.[11] Outside of device related programs owned and operated by Facebook are the companies that collect more personal data such as Masquerade, Moves, and Oculus. Masquerade is a facial recognition software, the data gathered through facial recognition points is retained to suggest who to tag in photos and Moves is an activity and exercise tracking devices that gathers user's identifying information from their body type, weight, and height.[12][13] Lastly, Oculus designs and creates virtual reality scenarios through imaging of real world areas.[14] The all of the information collected by these companies is permitted under the data and privacy policy to be shared within the Facebook family of companies. Table 1 outlines the types of data permitted to be shared outside of the Facebook family of companies.

Table 1. Data Permitted to be Shared outside of the Facebook Companies

Company	Identifying Data Shared:	Non-Identifying Data Shared:
Facebook	Yes	Yes
Facebook Payments	No	Yes
Atlas	Yes	Yes
Instagram, LLC	Yes	Yes
Onavo	Yes	Yes
Moves	Yes	Yes
Oculus	Yes	Yes
WhatsApp, Inc	Yes	Yes
Masquerade	Yes	Yes
Crowd Tangle	Yes	Yes

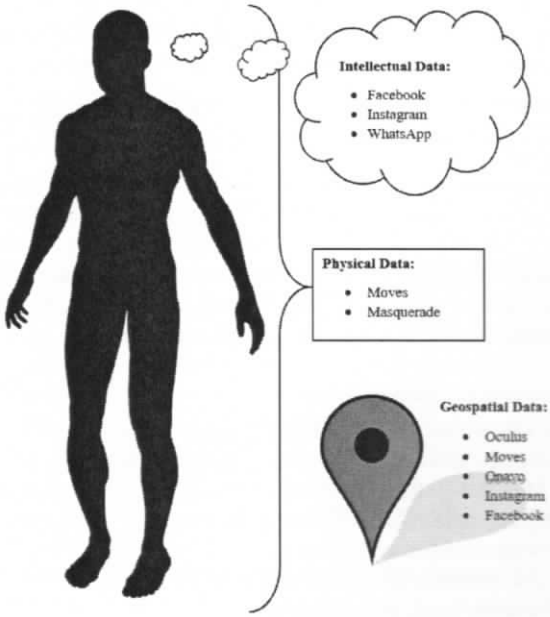
The Facebook companies are just one example of the massive amount of information that can be obtained, legally, on American citizens today. While unlikely, if a citizen was a member of Facebook and all nine of the Facebook

[11] *Privacy Policy.* (20 December 2013). Retrieved from Onavo: http://www.onavo.com/privacy_policy/#informationcollection
[12] *Privacy Policy.* (5 May 2014). Retrieved from Moves: http://moves-app.com/privacy
[13] *Privacy Policy.* (28 June 2016). Retrieved from Masquerade by Facebook: https://www.facebook.com/msqrd/privacy
[14] *Legal Documents.* (12 February 2016). Retrieved from Oculus: https://www.oculus.com/legal/privacy-policy

companies, that individual's privacy physically and intellectual would be at risk. Table 2 demonstrates an outline of how Facebook could pull together their data to form a copy of an individual right down to their habits and beliefs. This type of information collection is unrivaled by any non-government body in history, making the way in which America handles the challenge of protecting the privacy of Americans of the utmost important. While Americans are accepting these terms and conditions when creating an account there is no large label to tell an individual the potential risk, like there is on food and drugs. What is given to Facebook users is pages and pages of legal jargon claiming to aid in the user's security.

While the threat of social media may be seen as an issue only for younger generations to be more careful online, it also presents a threat to America's national security. With the gaps in local, state, and federal technological capabilities and equipment, the information held within governmental systems is still property of the United States Government. The information gathered by companies like Facebook are not tied to a nation, so without proper education and protection citizens could be handing their personal information over to an entity without the protection of the American Intelligence Community who is vulnerable to attacks or bribes by non-state actors.

Figure 1. Intellectual, Physical and Geospatial Data Is Collected Automatically



CONCLUSION

As we move further into the age of technology, there is no sign that the use of social media and the internet are declining. In this world revolving around clicks, likes, and shares personal information is readily available online. While these tools are valuable to our way of life and can be aids in improving the country, the public needs to be aware of the risk and the government needs to acknowledge the potential for damage. If the massive amount of identifying data stored in social media sites, like Facebook, were to fall into enemy hands the United States would face a crisis like none before. The enemies of the United States exploit these infrastructure weaknesses to collect intelligence while also utilizing the infrastructure to weaken our systems of intergovernmental self-governance.[15] While the American Intelligence Community has used the sea of personal information online to protect the country through open-source intelligence, the risk of American's personal information being used as a weapon or a cover identity is ever increasing. Americans need to be constantly aware of their online presence and demand action from the government to acknowledge and plan for social media as a potential threat to national security. Recent Congressional hearing on social media practices brought forth privacy concerns that mark the beginning of further investigation and expanded government oversight.[16] The privacy policies of social media companies are a civil rights and liberties issue for individual citizens as well as a national security concern.

---

[15] Hail, Michael W. "Federalism, Intergovernmental Relations, and Homeland Security." Book chapter in: Murray Bessette, Editor. *Liberty and Security in an Age of Terrorism*. Commonwealth Security Studies Laboratory: Xlibris, 177-186.

[16] Brown, Ryan. "Zuckerberg survived two days of grilling by Congress, but Facebook's troubles are not over yet." Last modified and published 2:20 AM ET Fri, 13 April 2018. https://www.cnbc.com/2018/04/13/after-zuckerberg-congress-hearing-facebook-awaits-further-scrutiny.html.

REFERENCES

Atlas. "Privacy Policy." Last modified April 13, 2015 https://atlassoulutions.com/privacy-policy/

Brown, Ryan. "Zuckerberg survived two days of grilling by Congress, but Facebook's troubles are not over yet." Last modified and published 2:20 AM ET Fri, 13 April 2018. https://www.cnbc.com/2018/04/13/after-zuckerberg-congress-hearing-facebook-awaits-further-scrutiny.html.

Crowd Tangle. "Privacy Policy." Last modified January 11, 2017 http://www.crowdtangle.com/privacy

Facebook. "Data Policy." Last modified September 29, 2016. https://www.facebook.com/about/privacy

Facebook Payments, Inc. "Privacy Policy." Last modified December 30, 2013. https://www.facebook.com/payments_payments_terms/privacy

Hail, Michael W. "Federalism, Privacy Rights, and Intergovernmental Management of Surveillance: Legal and Policy Issues." Book chapter in: *Video Surveillance*, edited by Weiyao Lin. Rijeka, Croatia: InTech Publishing, 2011, pp.27-34.

Hail, Michael W. "Federalism, Intergovernmental Relations, and Homeland Security." Book chapter in: Murray Bessette, Editor. *Liberty and Security in an Age of Terrorism.* Commonwealth Security Studies Laboratory: Xlibris, pp.177-186.

Instagram. "Privacy Policy." Last modified January 19, 2013. https://help.instagram.com/155833707900388

Masquerade. "Privacy Policy." Last modified June 28, 2016. https://www.facebook.com/msqrd/privacy

Moves. "Privacy Policy." Last modified May 5, 2014. http://moves-app.com/privacy

Nasr, Amir. Poll: Little Trust that Tech Giants will Keep Personal Data Private. Morning Consult. Last modified April 10, 2017. https://morningconsult.com/2017/04/10/poll-little trust-tech-giantswill-keep-personal-data-private/

Oculus. "Legal Documents." Last modified February 12, 2016 https://www.oculus.com/legal/privacy-policy

Onavo. "Privacy Policy." Last modified December 20, 2013 http://www.onavo.com/privacy_policy/#informationcollection

U.S. Department of Homeland Security. "Handbook for Safeguarding Sensitive Personally Identifiable Information." 2012.

WhatsApp. "WhatsApp Legal Info." Last modified August 25, 2016. https://www.whatsapp.com/legal/#privacypolicy