COMMENT: THE RECENT CLASHES AND COLLABORATIONS BETWEEN TECHNOLOGY COMPANIES AND THE U.S. GOVERNMENT IN SERVING NATIONAL SECURITY

Harrison Liangyu Fu[1]

I. INTRODUCTION

When it comes to serving national security in the digital age, the role that technology companies are playing has become more and more critical, presenting a challenge for the U.S. Government, in finding a way of reconciling the public interest for national security, as well as technology companies' private interest for privacy and independence. In recent years, the defense of national security is no longer limited in the traditional sense, where physical and tangible conflicts occur; rather, it has become intangible and often involves cyber security challenges fueled by the advance of technology.[2] In the matter of serving national security, the U.S. Government often requires cooperation and compliance from private technology giants, who often have firsthand or exclusive knowledge or access to help produce intelligence the U.S. Government needs to defend national security.[3]

---

[1] J.D. 2017, Albany Law School; B.S. 2014, Binghamton University. The author would like to thank Pershia Wilkins, David Pratt, Connie Mayer, Rosemary Queenan, Joann Fitzsimmons, Laurie Law, Nadia Castriota, Mary Walsh Fitzpatrick, Joanne Casey, Meg Wager, Colleen O'Byrne, David Singer, Corey Carmello, Eric Brenner, Matthew McNeill, Di Ma, Emmanuel Zamor, Lei Bo and Brenda Baddam for their continued support throughout his time at Albany Law School and beyond.

[2] *See* William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, U.S. DEP'T OF DEFENSE, http://archive.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx (last visited Nov. 18, 2016) (explaining that the traditional Cold War model of counter-attacking no longer apply in the modern cyber space sense).

[3] *See generally* Matt A. Mayer, *Gathering of National Security Team in Silicon Valley Signals Tech's Critical Role in Terrorism Fight*, AMERICAN ENTER. INST.

On the one hand, technology giants have the obligation and a corporate citizen's duty to aid the U.S. Government in gathering information under the USA Freedom Act[4] or the Foreign Intelligence Surveillance Act.[5] On the other hand, however, technology companies also need to maintain corporate responsibilities owed to its users and customers, in protecting their rights to privacy, as well as freedom of speech.

It is the balance of these two interests that creates a clash. This comment will mainly highlight those moments when clashes occur, and analyze those moments when collaborations take place, in the hopes of exploring remedies in law to further nurture the cooperation between technology companies and the U.S. Government in better serving national security.

II. CYBER SECURITY CHALLENGES IN NATIONAL SECURITY

According to the U.S. Department of Defense, over the past decade, the frequency and sophistication of intrusion in the U.S. military networks has increased exponentially.[6] The intensity has reached a point where "U.S. military and civilian networks are probed thousands of times and scanned millions of times" on a daily basis.[7] Since information technology is being heavily integrated with almost everything that the U.S. military does nowadays, from logistical support to global command and control of forces, real-time intelligence gathering to remote operations, the U.S. Government's reliance on computer networks potentially enables adversaries to gather valuable intelligence and subject the U.S. to cyber security vulnerabilities.[8] For example, the notorious 2008 cyber-attack on the U.S.,[9] which the Pentagon counter-

(Jan. 8, 2016), https://www.aei.org/publication/gathering-of-national-security-team-in-silicon-valley-signals-techs-critical-role-in-terrorism-fight/ (discussing national security team's efforts in bringing in Silicon Valley tech companies in fighting terrorism).

[4] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114–23, 129 Stat. 268 (2015).

[5] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95–511, 92 Stat. 1783 (1978) (codified as amended in scattered sections of 50 U.S.C.) [hereinafter *FISA*].

[6] Lynn, *supra* note 2.

[7] *Id.*

[8] *Id.*

[9] *Id.*

> In 2008, the U.S. Department of Defense suffered a significant compromise of its classified military computer networks. It began

attacked through "Operation Buckshot Yankee," is considered the worst breach of U.S. military computers in history,[10] which led to the creation of the United States Cyber Command.[11]

Moreover, cyber security threats to U.S. national security are not only limited to military targets, but also civilian infrastructures. Unfortunately, "[h]ackers and foreign governments are increasingly able to launch sophisticated intrusions into the networks that control critical civilian infrastructure."[12] This could lead to disastrous situations because civilian infrastructure is critical to the U.S.'s national security and homeland defense missions. Overall, the Department of Defense relies on the information technology infrastructure of the Country for its defense operations; thus, had the civilian infrastructure been directly targeted in a military conflict, or held hostage, to be used as bargaining chips against the U.S. Government, then any best-laid plans for defending the U.S. military networks would have meant little.[13] For instance, the U.S. military relies on civilian infrastructure to coordinate the deployment and resupply of the U.S. troops, provide troops with goods from private vendors, which would require the use of networks that are not Government-operated, both at home and abroad.[14] In addition, "computer-induced failures of U.S. power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption."[15] Thus, protecting civilian infrastructures and networks that undergird critical U.S. infrastructure is crucial

---

> when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control. It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary.

Id.

[10] *Id.* . . . .("This [attack] was the most significant breach of U.S. military computers ever, and it served as an important wakeup call. The Pentagon's operation to counter the attack, known as Operation Buckshot Yankee, marked a turning point in U.S. cyber defense strategy.").

[11] Cassandra M. Kirsch, *Science Fiction No More: Cyber Warfare and the United States*, 40 DENV. J. INT'L L. & POL'Y 620, 621 (2012).

[12] Lynn, *supra* note 2.

[13] *Id.*

[14] *Id.*

[15] *Id.*

for U.S. national security in the digital age.

However, when confronting these national security challenges, the U.S. Government cannot be, and should not be left to combat alone; rather, it also needs the allegiance from the private sector and partnership from technology companies. As the Defense Department eloquently and earnestly puts it, "[the] effort to defend the United States will only succeed if it is coordinated across the government, with allies, and with partners in the commercial sector."[16] Private commercial sectors and technology companies often enjoy a greater degree of freedom and flexibility when it comes to innovation, as opposed to the public sector.[17] For example, due to the inherent limitation of the government's complex administrative nature, the Pentagon needs "81 months to make a new computer system operational after it is first funded," whereas the iPhone was developed in merely 24 months.[18] Therefore, the U.S. Government often relies on technology companies in combatting cyber security challenges in defending national security. As the Assistant to President Obama for Homeland Security and Counterterrorism Lisa O. Monaco stated in her remarks[19] on strengthening the U.S.'s cyber defenses:

> To truly safeguard Americans online . . . we are going to have to work in lockstep with the private sector. . . . Partnership is a precondition of success. . . . The private sector has vital information we don't always see unless they share it with us, and the government has a unique capacity to integrate information about threats, including non-cyber sources, to create the best possible picture to secure all of our networks.20

She also reiterated President Obama's call for a conversation

---

16 *Id.*

17 *See generally* Kevin Merritt, *Can the Public Sector Outpace the Private Sector When it Comes to Innovation?*, U. OF WASH. (Jan. 24, 2016), http://www.washington.edu/innovation/2016/01/24/can-the-public-sector-outpace-the-private-sector-when-it-comes-to-innovation/ (explaining many public sector Chief Information Officers are financially chained and having trouble to invest in innovation technologies).

18 Lynn, *supra* note 2.

19 Office of the Press Secretary, *Remarks as Prepared for Delivery by Assistant to the President for Homeland Security and Counterterrorism Lisa O. Monaco Strengthening our Nation's Cyber Defenses*, WHITE HOUSE (Feb. 10, 2015), https://www.whitehouse.gov/the-press-office/2015/02/11/remarks-prepared-delivery-assistant-president-homeland-security-and-coun.

20 *Id.*

among Americans on "how the government can use as much data as possible to track and arrest hackers," while at the same time recognizing technology companies like Apple and Google's need for privacy and room for independent encryption development efforts.[21] As a result, it is in the balance of the two interests—U.S. Government's demand for technology companies' cooperation, in producing intelligence pertinent to national security, versus, technology companies' need for privacy, independence, and maintaining responsibilities for their customers—that clashes occur.

III. U.S. GOVERNMENT'S NEEDS FOR ASSISTANCES FROM TECHNOLOGY GIANTS

As noted previously, the U.S. Government's need for technology companies' assistances in serving national security is just as necessary as it is compulsory. In 2013, in the wake of Edward Snowden's unauthorized disclosures of classified information from the U.S. Government, which revealed numerous global surveillance programs and government secrecy that were otherwise top-secret, members of the Congress believed legislative changes were needed to restore public trust.[22] The balance between the need for information privacy and national security called for the enactment of the USA Freedom Act of 2015. The objective of this act is:

> To rein in the dragnet collection of data by the National Security Agency (NSA) and other government agencies, increase transparency of the Foreign Intelligence Surveillance Court (FISC),

---

[21] *See* Tom Risen, *New Agency to Aid in Battle Against Hackers: The Creation of a New Cybersecurity-Centered Government Agency Echoes Post-9/11 Efforts to Fight Terrorism*, U.S. NEWS (Feb. 10, 2015), http://www.usnews.com/news/articles/2015/02/10/new-cybersecurity-agency-to-aid-in-battle-against-hackers ("Google and Apple each said last year that they would encrypt their smartphones so they could not be compelled by law enforcement to unlock information stored on the devices, raising concerns from both FBI Director James Comey and Obama about whether that would hinder law enforcement investigations.").

[22] *See* Dan Roberts, *Patriot Act Author Prepares Bill to Put NSA Bulk Collection "Out of Business"*, GUARDIAN (Oct. 10, 2013), https://www.theguardian.com/world/2013/oct/10/nsa-surveillance-patriot-act-author-bill ("Many lawmakers have agreed that some new legislation is required in the wake of the collapse in public trust that followed Snowden's disclosures, which revealed how the NSA was collecting bulk records of all US phone calls in order to sift out potential terrorist targets.").

> provide businesses the ability to release information regarding FISA requests, and create an independent constitutional advocate to argue cases before the FISC.[23]

FISC was established under FISA, which is a special U.S. Federal Court that holds nonpublic sessions to consider the issuance of warrants pursuant to FISA. Notably, all proceedings before FISC are *ex parte*, meaning that U.S. Government is the only party present.[24] FISA was enacted as a result of the congressional investigations into Federal surveillance activities that were conducted in the name of national security.[25] Through the mechanism of FISA, Congress intended to provide "judicial and congressional oversight of foreign intelligence surveillance activities while maintaining the secrecy necessary to effectively monitor national security threats."[26]

In modern days, through amendments since 1978, FISA has established procedures for "the authorization of electronic surveillance, use of pen registers and trap and trace devices, physical searches, and business records for the purpose of gathering foreign intelligence."[27] As the plain text demonstrates, FISA provides very broad authority for the U.S. Government to gather foreign intelligence. Similarly, as a result of the USA Freedom Act of 2015, although past governmental practices such as bulk collection of phone records were outlawed, U.S. intelligence agencies still retain broad authority in information collecting on potential terrorists.[28] In the combat against terrorism and in defending national security in this digital age, fortunately, the U.S. Government and the technology companies share a common understanding: the latter's cooperation is essential and irreplaceable, especially in the area of domestic surveillance

---

[23] Jim Sensenbrenner, *THE USA FREEDOM ACT*, U.S. HOUSE OF REPRESENTATIVES, http://sensenbrenner.house.gov/legislation/theusafreedomact.htm (last visited Nov. 20, 2016).

[24] Bureau of Justice Assistance, *The Foreign Intelligence Surveillance Act of 1978 (FISA)*, U.S. DEPARTMENT OF JUSTICE (Sept. 19, 2013), https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] Ed Ferrara, *5 Things You Need to Know About the USA Freedom Act*, NEXTGOV (June 5, 2015), http://www.nextgov.com/technology-news/tech-insider/2015/06/what-you-need-know-about-usa-freedom-act/114601.

activities.[29] For example, this relationship can be evidenced by the closed-door summit between the White House and technology giants that took place in early 2016 on combating Islamic State terrorism:

> The remarkable rendezvous between Apple, Facebook, Twitter, Microsoft and others and a delegation from the White House revealed a willingness on the part of tech firms to work with the government, and indicated that the Obama administration appears to have concluded it can't combat terrorists online on its own.[30]

Nevertheless, the relationship between the two is not always harmonious or without conflicts. Instead, their interests often collide, and in the balance of the two, clashes occur.

VI. CLASHES BETWEEN TECHNOLOGY COMPANIES AND THE U.S. GOVERNMENT IN THE INTEREST OF NATIONAL SECURITY

A. Twitter's Battle Against the U.S. Government for More Transparency

Twitter, as one of the technology giants that the U.S. Government relies on in collecting intelligence pertinent to national security, is also a pioneering free speech advocate.[31] In early October of 2014, Twitter sued the U.S. Department of Justice, defending its freedom and right of disclosing additional information regarding the kinds of data that U.S. Government sought from Twitter users.[32] Twitter wanted to present its users more detailed information in its transparency report, particularly the number of FISA orders and National Security Letters ("NSLs") it received from the U.S. Government.[33] Such orders would allow

---

[29] *Id.* ("There is a general understanding that the FBI and NSA cannot conduct their domestic surveillance activities without the assistance of U.S. companies. The reality is the private sector controls most of the cyberinfrastructure the FBI and NSA need to conduct surveillance.").

[30] Danny Yadron et al., *Silicon Valley Appears Open to Helping US Spy Agencies after Terrorism Summit*, THE GUARDIAN (Jan. 8, 2016), https://www.theguardian.com/technology/2016/jan/08/technology-executives-white-house-isis-terrorism-meeting-silicon-valley-facebook-apple-twitter-microsoft#top.

[31] Victor Luckerson, *Twitter Is Suing the Government So it Can Tell You More About Surveillance*, TIME (Oct. 7, 2014), http://time.com/3479012/twitter-suing-department-justice.

[32] *Id.*

[33] *Id.*

the Government to secretly gather communication data that it deems pertinent to national security threats, and recipients of such order requests are prohibited from disclosing that they have received them.[34]

In fact, the U.S. Government actually afforded technology companies a certain degree of freedom in disclosing permissible information. However, such restrictions did not align with Twitter's values. For instance, technology giants may report the numbers of Government requests they received in broad bands, such as from zero to 999; however, Twitter wanted to report "the exact number of national-security-related orders received in any particular category."[35] Without a doubt, this objective directly clashed with the Government's goal in keeping these data confidential: the National Security Agency and the FBI, often operating under secretive protocols, need confidentiality and integrity of these data to effectively protect the country from real security threats.[36] Without the outer-layer protection that the non-disclosure restriction affords, the adversaries would have gauged the Government's intentions and missions in advance, compromising any preventative or counteroffensive measures put by the Government in its inner-core; in other words, the Government believed that the less that the world knows about the mechanism and sources through which it collects intelligence, the better its chances of persevering its capabilities and thus better defending national security.[37]

The U.S. Government was at a difficult spot to be in. However, this does not mean that it was not willing to make compromises. In fact, in responding to Twitter's demand, the Justice Department attempted to reach a reasonable middle ground that allowed a greater level of disclosure while shielding its ability to protect national security.[38] Nevertheless, Twitter felt that waiting for the Government to voluntarily give up upon, or reduce its restrictive regulations would be a wish that may take years to come; thus, it

---

[34] *Id.*

[35] Ellen Nakashima, *Twitter Sues U.S. Government over Limits on Ability to Disclose Surveillance Orders*, WASH. POST (Oct. 7, 2014), https://www.washingtonpost.com/world/national-security/twitter-sues-us-government-over-limits-on-ability-to-disclose-surveillance-orders/2014/10/07/5cc39ba0-4dd4-11e4-babe-e91da079cb8a_story.html?utm_term=.f38098c42789.

[36] *Id.*

[37] *Id.*

[38] *See id.*

sought remedies in court.[39] Illustrating the underlying reasons for Twitter's taking legal action against the U.S. Government: "In a post-Edward Snowden world in which technology companies are striving to reassure customers about their commitment to privacy, Twitter is pressing for the ability to be more candid in its twice-a-year transparency reports than the government has been willing to permit."[40]

Before this legal clash took place, Twitter actually tried on multiple occasions communicating with the Government, expressing its aspiration to provide more transparency to its users and voicing its concerns for the corresponding governmental restrictions.[41] In addition, Twitter also submitted the draft transparency report to the Government on April 1, 2014, requesting "a determination as to exactly which, if any, parts of its Transparency Report are classified or, in the [government's] view, may not lawfully be published online."[42] However, the Justice Department did not address Twitter's concerns within a reasonable time frame.[43] About five months later, on September 9, 2014, the Government responded to Twitter that "'information contained in the report is classified and cannot be publicly released' because it does not comply with the Government's approved framework for reporting data about FISA orders and NSLs."[44] However, in its response, the Government did not provide guidance as to what sort of language in the draft transparency report was appropriate to be disclosed or not.[45] Having exhausted all of its venues in hoping to achieve a common ground with the U.S. Government, yet with fruitless result, according to Twitter, it had not choice but to seek a remedy in court.[46] Specifically, in its

---

39 Twitter, Inc. v. Lynch, 139 F. Supp. 3d 1075, 1078–79 (N.D. Cal. 2015) ("Twitter filed its Complaint herein on October 7, 2014.").

40 Nakashima, *supra* note 35.

41 Jeremy Kessel, *Continuing Our Fight for More #Transparency*, TWITTER (July 31, 2014), https://blog.twitter.com/2014/continuing-our-fight-for-more-transparency ("[e]arlier this year we met with officials from the United States Department of Justice [] and the Federal Bureau of Investigation [] in Washington to push for our ability to provide greater transparency concerning national security requests.").

42 Twitter, Inc., 139 F. Supp. 3d at 1078–79.

43 *Kessel, supra* note 40 ("[o]ver 90 days have passed, and we still have not received a reply. Therefore, we are weighing our legal options to provide more transparency to our users.").

44 Twitter, Inc., 139 F. Supp. 3d at 1078–79.

45 *Id.*

46 Benjamin Lee, *Taking the Fight for #Transparency to Court*, TWITTER (October 7, 2014), https://blog.twitter.com/2014/taking-the-fight-for-

public statement, Twitter averred that its First Amendment right was infringed upon by governmental restrictions:

> Our ability to speak has been restricted by laws that prohibit and even criminalize a service provider like us from disclosing the exact number of [requests] received. . . . So, today, we have filed a lawsuit in federal court seeking to publish our full Transparency Report, and asking the court to declare these restrictions on our ability to speak about government surveillance as unconstitutional under the First Amendment.[47]

Twitter's First Amendment claim contained two Counts in its amended complaint, with Count I challenging Government's FISA nondisclosure provisions as "prior restraints of indefinite duration" on its face, and Count II contending them to be unconstitutional as applied.[48] The court ultimately ruled for the Government, pursuant to the principal set forth by the U.S. Supreme Court that "The First Amendment does not permit a person subject to secrecy obligations to disclose classified national security information."[49]

Therefore, by its reasoning, the court held that since Twitter did not allege Government's categorization of the restricted information as "classified," Twitter had no viable claim; to the contrary, Twitter in fact conceded that the aggregated data, regarding Twitter's receipt of the legal process under the FISA order, was classified.[50] As for Twitter's Count I allegation, the Court explained that Twitter's argument "does not take into account the fact that a classification decision is necessarily limited in duration by its nature."[51] As for Twitter's Count II allegation, the Court reasoned that Twitter's constitutional challenge against the FISA nondisclosure provisions "does not account for the fact

---

transparency-to-court.

> We've tried to achieve the level of transparency our users deserve without litigation, but to no avail. In April, we provided a draft Transparency Report addendum to the U.S. Department of Justice and the Federal Bureau of Investigation, a report which we hoped would provide meaningful transparency for our users. After many months of discussions, we were unable to convince them to allow us to publish even a redacted version of the report.

Id.

47 *Id.*

48 Twitter, Inc. v. Holder, 183 F. Supp. 3d 1007, 1014 (N.D. Cal. 2015).

49 *Id.* (citing Snepp v. United States, 444 U.S. 507, 509 n. 3 (1980)).

50 *Id.*

51 *Id.*

that the Government has refused to permit disclosure of the aggregate numbers on the grounds that the information is classified pursuant to the Executive Order (not because of any FISA order or provision)."[52]

Had Twitter challenged Government's categorization of the draft transparency report, which if considered as "classified" and thus constituted national security information, it may have standing on its constitutional claim and then be eligible to seek appropriate remedies. Since Twitter failed to allege so, it did not possess a viable First Amendment claim.[53] Other technology companies can certainly learn from Twitter's case and strategize future actions that are similarly situated, challenging the Government's classification scheme and avoiding legal impasses. Although Twitter did not prevail on its constitutional claims, this legal battle nevertheless exemplified the type of tension between modern technology companies and the U.S. Government when it comes to serving the interest of national security.

B. A Modest Victory from Other Technology Giants in the Fight Against Governmental Restrictions

Twitter was not alone in this battle. Other technology companies also voiced their dissatisfactions about the governmental restrictions on their freedom and ability of providing better transparency to their users. Among these companies were Google, Facebook, Yahoo, LinkedIn and Microsoft,[54] whose fight preceded Twitter's and provided a basis for Twitter's subsequent legal action. In 2013, these major technology firms sought permission to disclose more detailed information regarding national security related requests they received from the U.S. Government, including "the aggregate number of user accounts affected and the statutory authority for these orders."[55] After the Government refused to provide such flexibility, these companies

---

[52] *Id.*

[53] *Id.* ("In the absence of a challenge to the decisions classifying that information, Twitter's Constitutional challenges simply do not allege viable claims.").

[54] Naomi Gilens, *Note: The NSA Has Not Been Here: Warrant Canaries as Tools for Transparency in the Wake of the Snowden Disclosures*, 28 HARV. J. LAW & TECH. 525, 527–28 (2015) ("Information released about the government's collection of user data from communications providers also generated a strong public demand for companies to become more transparent with information regarding how user information is shared with the government.").

[55] *Id.* at 528.

sued in the secret Foreign Intelligence Surveillance Court, challenging the restriction.[56]

However, a settlement outside the secret FISA court was finally reached where the Government agreed to relax the nondisclosure restrictions to a certain degree, "but companies' freedom to share information with the public remains cabined by stringent limitations."[57] According to such settlement, the new policy will permit these companies to disclose national security letters, essentially a form of administrative subpoenas, as well as the FISA requests; technology companies were prohibited from doing so previously because the Government was concerned that the disclosure might compromise its efforts in combating national security threats.[58]

As discussed previously, however, the permitted disclosure was only limited to the disclosure of the number of requests in wide numerical ranges.[59] There are also additional restrictions. For instance, a communication service provider, such as these five technology companies, can only publish FISA and NSL numbers every six months, meaning that companies would have to wait six months before they could submit another request to include new data for the corresponding period.[60] Additionally, this settlement also imposes another two-year delay on the providers' ability to disclose the type of data that are essentially a matter of first impression.[61] This settlement was of course not without criticism among the civil-liberties advocate communities. The New America Foundation, for example, commented that such agreement, by "[f]uzzing the numbers into ranges of a thousand . . . serves no national security purpose while making it impossible to effectively evaluate how those powers are being used."[62] On the bright side,

---

56 *Id.*

57 *Id.*

58 Craig Timberg & Adam Goldman, *U.S. To Allow Companies To Disclose More Details on Government Requests for Data*, WASH. POST (Jan. 27, 2014), http://www.washingtonpost.com/business/technology/us-to-allow-companies-to-disclo-semore-details-on-government-requests-for-data/2014/01/27/3cc96226-8796-11e3-a5bd-844629433ba3_story.html ("The Justice Department has agreed to relax its long-standing gag order on certain types of data requests made to companies, allowing them for the first time to publicize—in broad terms—how much customer information they must turn over to the government. . . .").

59 *Id.*

60 Letter from James M. Cole, Deputy Attorney Gen., to Colin Stretch, Vice President and Gen. Counsel, Facebook, et al. (Jan. 27, 2014), http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf.

61 *Id.*

62 Sam Gustin, *Watchdogs: NSA Tech Data Deal Doesn't Go Far Enough*, TIME

however, this settlement was nevertheless a "commendable" progress that many advocates embraced dearly.[63]

On the Government's end, the Justice Department was only willing to make such compromise after the office of the Director of National Intelligence's careful consulting with other departments and agencies.[64] The Government determined that through the disclosure of the aggregate data information, the public interest served would outweigh the national security concerns that previously demanded such data's classification status.[65] Therefore, as part of the settlement agreement, the technology giants dropped their respective lawsuits before the Foreign Intelligence Surveillance Court, the goal of which was a demand for greater transparency, which to a certain degree was realized through the settlement.[66] The companies were satisfied with the result and issued a joint statement acknowledging their position with the policy change, expressing that they will "continue to encourage Congress to take additional steps to address all of the reforms [they] believe are needed."[67]

This result marked a modest victory for leading technology

(Jan. 28, 2014), http://business.time.com/2014/01/28/nsa-tech-transparency-deal.

[63] *Google, Facebook, And Other Tech Firms Will Be Allowed To Release Info About NSA Requests*, AM. CIV. LIBERTIES UNION (Jan. 27, 2014), https://www.aclu.org/news/google-facebook-and-other-tech-firms-will-be-allowed-release-info-about-nsa-requests?redirect=national-security/google-facebook-others-will-be-allowed-release-info-about-nsa-requests.

> Companies must be allowed to report basic information about what they're giving the government so that Americans can decide for themselves whether the NSA's spying has gone too far. It is commendable that the companies pressed the government for more openness, but even more is needed. Congress should require the government to publish basic information about the full extent of its surveillance, including the significant amount of spying that happens without the tech companies' involvement.

Id.

[64] Timberg & Goldman, *supra* note 58.

[65] *Id.*

[66] Andrea Chang & Paresh Dave, *Twitter Sues U.S. Government Over Surveillance Disclosure Rules*, L.A. TIMES (Oct. 7, 2014), http://www.latimes.com/business/la-fi-twitter-sues-doj-fbi-20141008-story.html.

[67] Microsoft News Center, *Response to U.S. Government Announcement on Increased Transparency Regarding National Security Orders*, MICROSOFT (Jan. 27, 2014), https://news.microsoft.com/2014/01/27/response-to-us-government-announcement-on-increased-transparency-regarding-national-security-orders/#tE0iDIEGfqmiU1rd.99 ("We filed our lawsuits because we believe that the public has a right to know about the volume and types of national security requests we receive. We're pleased the Department of Justice has agreed that we and other providers can disclose this information.").

companies, in their legal battle with the U.S. Government, regarding their freedom and obligations in disclosing information under certain restrictive governmental surveillance programs and regulations.

C. Apple's Fight to Protect User Privacy Against the U.S. Government's Request for National Security

In a horrific terrorist attack that took place in December 2015 in San Bernardino, California, where 14 people were killed, the essential evidence that the Justice Department needed to extract involved an iPhone used by one of the attackers.[68] As the manufacturer of the iPhone, Apple possessed the capability to unlock the iPhone that otherwise remained encrypted; the Federal Bureau of Investigation ("FBI") sought Apple's assistance, hoping Apple would help unlock the encrypted iPhone.[69] However, Apple declined to assist the U.S. Government in unlocking the iPhone, citing concerns that establishing such a precedent would lead to future Government efforts to request Apple to unlock even more iPhones owned by users for criminal prosecution cases.[70] As Apple's CEO Tim Cook stated in response to the Government's demand: "The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand."[71] According to Apple, the U.S.

---

[68] Eric Lichtblau & Joseph Goldstein, *Apple Faces U.S. Demand to Unlock 9 More iPhones*, N.Y. TIMES (Feb. 23, 2016), https://www.nytimes.com/2016/02/24/technology/justice-department-wants-apple-to-unlock-nine-more-iphones.html.

[69] *Id.* ("In the San Bernardino case, prosecutors have cast their demands for Apple to help them unlock the iPhone used by Syed Rizwan Farook—one of the attackers in the December rampage, in which 14 people were killed—as a limited effort in response to an unusual situation."). *See also* Mike Isacc, *Explaining Apple's Fight With the F.B.I.*, N.Y. TIMES (Feb. 17, 2016), https://www.nytimes.com/2016/02/18/technology/explaining-apples-fight-with-the-fbi.html.

> The Federal Bureau of Investigation wants to examine the iPhone used by Syed Farook to determine whether he and his wife, Tashfeen Malik, had planned the shooting directly with the Islamic State. Apple would have to build a new version of its iOS smartphone software that allows the F.B.I. to bypass certain restrictions.

Id.

[70] Issac, *supra* note 69.

[71] Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/.

Government was essentially asking it to hack its own users, which would undermine their decades of security efforts that were intended to protect user confidentiality.[72] Additionally, Apple was afraid that, by submitting to the Government's request, in creating such a tool—which the Government maintained to be a one-time use only case—it would subject itself to future risks where the tool could be used over and over again in serving government's future needs.[73]

Without the legislative authority that directly governed the encryption controversy, the FBI sought authority under the All Writs Act of 1789 ("AWA"),[74] which states "[a]ll courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[75] Such a practice was considered to be very extraordinary. The U.S. Supreme Court recognized the power conferred under the AWA in its 1977 decision in *United States v. New York Tel. Co.*.[76] However, such power was intended to be more of a narrow exception under extraordinary circumstances than otherwise.[77] The Court essentially constructed a three-factor test governing governmental authority derived under the AWA, which was construed by the public as "to preserve its important balance between flexibility and tyranny."[78] The Court expressed its concerns about the need to limit the authority under AWA: "We agree that the power of federal courts to impose duties upon third parties is not without limits; unreasonable burdens may not be

---

[72] *Id.*

[73] *Id.* ("In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks—from restaurants and banks to stores and homes. No reasonable person would find that acceptable.").

[74] 28 U.S.C. § 1651 (2012). *See* Amy Davidson Sorkin, *The Dangerous All Writs act Precedent in the Apple Encryption Case*, NEW YORKER (Feb. 19, 2016), https://www.newyorker.com/news/amy-davidson/a-dangerous-all-writ-precedent-in-the-apple-case.

[75] 28 U.S.C. § 1651.

[76] United States v. N.Y. Tel. Co., 434 U.S. 159, 172, 174 (1977).

[77] Neil Richards & Woodrow Hartzog, *Apple V The FBI: Why The 1789 All Writs Act Is The Wrong Tool*, THE GUARDIAN (Feb. 24, 2016), https://www.theguardian.com/technology/2016/feb/24/apple-v-the-fbi-why-1789-all-writs-act-is-the-wrong-tool ("They give the government the power to do its job in a way that is flexible but constrained by law. They are exceptions to the rule that all powers must be spelled out and, as exceptions, they must not be allowed to swallow the rule.").

[78] *Id.* ("A sensible, safe internet requires that we be able to trust the tech companies with whom we entrust the data of our digital lives. The narrow exception of the AWA should not be allowed to swallow the rule that government power is flexible but limited.")

imposed."[79] Simply put, in order for the power conferred under AWA to be lawful, the company being ordered to comply with the governmental request must "(1) be related and not 'removed' from the case; (2) the order must not place an unreasonable burden on the company; and (3) the company's assistance must be necessary."[80] Therefore, a plain read and application of this test would yield a conclusion that Apple was not a party under FBI's investigation; the burden placed on Apple would be extremely burdensome, as hacking its own customers was contrary to Apple's values; and Apple's assistance was not absolutely necessary, as the Government could seek alternative means to extract the information on Apple's iPhones.

As it turned out, an order issued by a Magistrate Judge of the Federal District Court for the Central District of California directed Apple to bypass its security system in an effort to assist the FBI in obtaining access to the data.[81] However, in this balance between the U.S. Government's interest in serving national security and Apple's corporate responsibility in upholding its values and protecting users' privacy, Apple stood its ground, determined to fight for what it believed in. Apple argued that the scope of this Act needed to be limited, citing a 2005 Magistrate Judge Order, which rejected the argument that this Law can be applied in compelling a telecommunications provider to allow real-time tracking of a cellphone, absent a search warrant.[82]

Specifically, in Apple's favor, the U.S. District Court for the Eastern District of New York ruled "the All Writs Act did not provide the legal authority to require Apple Inc. to bypass the encrypted lockscreen passcode of an iPhone for the federal government in order to execute a search warrant."[83] The Court reasoned that, "under a more appropriate understanding of the [AWA] function as a source of residual authority . . . the relief the

---

79 N.Y. Tel. Co., 434 U.S. at 172.

80 Richards, *supra* note 77.

81 Eric Lichtblau and Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html ("The government says the law gives broad latitude to judges to require "third parties" to execute court orders. It has cited a 1977 ruling requiring phone companies to help set up a pen register, a device that records all numbers called from a particular phone line.").

82 *Id.*

83 John Potapchuk, *A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data Under the All Writs Act*, 57 B.C. L. REV. 1403, 1403 (2016).

government seeks is unavailable because Congress has considered legislation that would achieve the same result but has not adopted it."[84] In addition, after considering the factors set forth by the U.S. Supreme Court in deciding whether an order under the AWA is appropriate, the Court determined that none of the three factors[85] were met in justifying the imposition of obligation on Apple for it to assist the U.S. Government's investigation effort against its own freewill.[86] Therefore, this decision basically stripped the Government of an investigative tool that it had routinely relied upon.[87]

Although Apple fought hard against this request from the U.S. Government, it has always been proactive in helping the latter in gathering necessary data, within the boundaries of maintaining its responsibilities to its users and upholding its values. For example, Apple had long held a position that it would hand over data to comply with a court order when it was technically capable of doing so.[88] To put it statistically, from Apple's Report covering the first half-year of 2015, it contended to have received approximately 27,000 requests from all governmental agencies around the world for data on about 363,000 devices.[89] Apple provided some of that data in about 16,000 instances.[90]

Apple has made its position clear: that it believes that national security should not come at the expense of an individual's privacy.[91] In addition, provided that Apple could freely provide transparency and create dialogues to cope with the overarching impact from surveillance laws and regulations, it is also committed to engage with the governments, legislators, and courts worldwide, on the important issue of ensuring user data privacy and security.[92] This is what Apple believes in. Apple's privacy policy states:

---

84 *In re* Apple, Inc., 149 F. Supp. 3d 341, 344 (E.D.N.Y. 2016).

85 *Id.* ("[t]he closeness of Apple's relationship to the underlying criminal conduct and government investigation; the burden the requested order would impose on Apple; and the necessity of imposing such a burden on Apple.").

86 *Id.*

87 Gustin, *supra* note 62.

88 *Privacy*, APPLE (last visited Feb. 9, 2017), http://www.apple.com/privacy/government-information-requests/.

89 *Report on Government Information Requests: January 1-June 30, 2015*, APPLE (2015), https://www.apple.com/legal/privacy/transparency/requests-20150914-en.pdf.

90 *Id.*

91 Gustin, *supra* note 62.

92 *Id.*

> Apple requires government and private entities to follow applicable laws and statutes when requesting customer information and data. We contractually require our service providers to follow the same standard we apply to government information requests for Apple data. Our legal team reviews requests to ensure that the requests have a valid legal basis. If they do, we comply by providing the narrowest possible set of data responsive to the request. If they do not have a valid legal basis, or if we consider it to be unclear, inappropriate, or overly broad, we challenge or reject the request.[93]

Although the FBI did not prevail against Apple in its attempt to compel Apple to produce the intelligence it hardly needed in serving national security interests, the FBI nevertheless wound up finding an alternative, in unlocking the iPhone in controversy. The Justice Department announced in late March 2016 that it had found a way of unlocking an iPhone without Apple's help, which allowed it to withdraw the legal effort to compel Apple to assist it in a mass-shooting investigation.[94] In light of Apple's heated resistance and the media attention this battle had drawn, the debate between whether national security or privacy was more important still remains a question for all to see.[95]

V. COLLABORATIONS BETWEEN TECHNOLOGY COMPANIES AND THE U.S. GOVERNMENT IN THE INTEREST OF NATIONAL SECURITY

A. Yahoo's Accommodation of U.S. Government's Need for Surveillance

Despite fierce clashes with the U.S. Government, at times, technology giants are at the frontier of assisting the latter to conquer challenges that the latter could not solve alone. Yahoo's latest cooperation with the U.S. Government in 2016 serves as a leading example.

In light of Yahoo's long overdue finding of its computer network breach, which took place in 2014 and compromised credentials of approximately 500 million users, two weeks after such discovery,

---

93 *Id.* ("Apple has never worked with any government agency from any country to create a "backdoor" in any of our products or services. We have also never allowed any government access to our servers. And we never will.").

94 Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (Mar. 28, 2016), https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html.

95 *Id.*

Yahoo elected to comply with a secret court order from the Foreign Intelligence Surveillance Court.[96] Pursuant to this order, Yahoo was required to search for messages that contain a computer signature specifically tied to communications of a terrorist organization.[97] The underlying justification for the issuance of this order was that there was probable cause indicating that the digital signature via Yahoo's email service was uniquely utilized by a foreign power for a terrorist organization.[98] The Government spokesperson commented that orders under FISA, such as the one for Yahoo, would not involve bulk collection of user data or indiscriminately review email communications of ordinary users.[99] Instead, according to the spokesperson, such orders are narrowly construed and merely focused on collecting signals intelligence. In Yahoo's case, for example, this meant providing leads to terrorists' communications.[100]

Yahoo complied and customized an existing screening system for its incoming email traffic, for which Yahoo maintained that it only "narrowly interpret[s] every government request for user data to minimize disclosure."[101] Yahoo's cooperation is without a doubt a great contribution to the Government so that the latter can better defend national security and combat terrorism. Without Yahoo's willingness to provide such intelligence, the Government would not be able to intercept terrorism communications that took place on Yahoo's network, nor could it effectively deter potentially dangerous and radical actions from commencing.

Nevertheless, Yahoo's decision also opened the public debate over the trade-offs between Internet users' privacy rights and the need for security. An American Civil Liberties Union attorney expressed disappointment over Yahoo's decision of not challenging the FISA surveillance order, lamenting that Yahoo users were counting on it to stand up against the spying demands from the

---

96 Charlie Savage & Nicole Perlroth, *Yahoo Said to Have Aided U.S. Email Surveillance by Adapting Spam Filter*, N.Y. TIMES (Oct. 5, 2016), https://www.nytimes.com/2016/10/06/technology/yahoo-email-tech-companies-government-investigations.html?_r=0.

97 *Id.*

98 *Id.* ("Investigators had learned that agents of the foreign terrorist organization were communicating using Yahoo's email service and with a method that involved a 'highly unique' identifier or signature, but the investigators did not know which specific email accounts those agents were using. . . .").

99 *Id.*

100 *Id.*

101 *Id.*

Government, especially the one at hand.[102] On the other hand, in response to the criticism against Yahoo for having "secretly built a custom software program to search all of its customers' incoming emails for specific information provided by U.S. intelligence officials,"[103] Yahoo rejected such allegation and maintained that the alleged scanning system did not exist.[104] Additionally, FISA experts who defended Yahoo's decision to comply contended that the surveillance court has the authority to obtain data from a search for a specific term, so long as it is not a search for a specific account.[105]

What makes technology companies' situation especially difficult, as in Yahoo's case, is that often times they cannot clarify details of their decision when cooperating with the Government. As discussed in the previous section, Twitter's fight for transparency exemplifies the exact dilemma facing technology companies, when it comes to the degree of freedom they have, in disclosing governmental surveillance information to their users. Yahoo's cooperation with the U.S. Government should be celebrated in a sense that, at least on its surface, it will assist the Government to serve national security without compromising users' privacy on a massive scale. Nevertheless, technology companies complained about their inability to "explain to customers what sort of data they do and do not turn over"[106] under the FISA order. Therefore, this challenge rests with the legislature, who needs to figure out a way of helping the Government maintain a healthy and mutually beneficial relationship with technology companies, whose cooperation the former cannot afford to forfeit when serving national security.

---

[102] Joseph Menn, *Exclusive: Yahoo secretly scanned customer emails for U.S. intelligence – sources*, REUTERS (Oct. 4, 2016), http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT. *See also ACLU Comment on Yahoo Email Scanning*, AMERICAN CIV. LIBERTIES UNION (Oct. 4, 2016), https://www.aclu.org/news/aclu-comment-yahoo-email-scanning ("[T]he order issued to Yahoo appears to be unprecedented and unconstitutional. The government appears to have compelled Yahoo to conduct precisely the type of general, suspicionless search that the Fourth Amendment was intended to prohibit.").

[103] *Id.*

[104] Savage, *supra* note 96.

[105] Menn, *supra* note 102 ("[The] 'upstream' bulk collection from phone carriers based on content was found to be legal . . . and the same logic could apply to Web companies' mail.").

[106] Savage, *supra* note 96.

B. Tech Giants Declare War on Terrorism as Desired by the U.S. Government

In January 2016, the White House invited executives from leading technology companies for a summit to discuss ways of deterring ISIS terrorism and urged tech giants to help in their respective roles.[107] Tech firms including Apple, Facebook, Google, LinkedIn, Microsoft and Twitter, joined President Obama's Chief of Staff, the Director of National Intelligence, and officials from the Justice Department at the conference, exchanging thoughts and voices on counterterrorism.[108] One key issue discussed was about the means of tracking radical extremists online, which the U.S. Government hoped tech giants could assist and urged them to develop techniques that would detect and measure radicalization.[109] Since terrorists often utilize social media for expansion, the Government was concerned that terrorists are able to leverage the Internet for recruiting, radicalizing, and mobilizing followers for violence.[110] In contrast, technology companies, as service providers, have the exclusive ability to detect such behaviors and their online declaration of war on terrorism is an ally gesture that the U.S. Government longs for long.

In fact, even prior to this summit, both the House and the Senate had already recognized the importance of a concerted collaboration between the Government and technology companies in the fight against terrorism. Congress hopes to facilitate this process, which not only expects federal agencies to step up their game in future counterterrorism efforts, but also demands providers of Internet communications to be more responsive.

---

[107] Jose Pagliery & Laurie Segall, *White House Asks Silicon Valley to Help Silence ISIS Online*, CNN (Jan. 2016), http://money.cnn.com/2016/01/08/technology/white-house-isis-silicon-valley?iid=EL.

[108] *Id.*

[109] *Id.*

[110] Hugh Handeyside, *Social Media Companies Should Decline the Government's Invitation to Join the National Security State*, JUST SECURITY (Jan. 2016), https://www.justsecurity.org/28755/social-media-companies-decline-governments-invitation-join-national-security-state/ ("The pressure on social media companies to limit or take down content in the name of national security has never been greater.").

VI. CONGRESSIONAL EFFORTS AND OTHER POSSIBLE MEANS TO PROTECT NATIONAL SECURITY

The House introduced a bill on September 30, 2015 called the Combat Terrorist Use of Social Media Act of 2015,[111] which demands "a report on United States strategy to combat terrorist use of social media" from the executive branch.[112] The proposed legislation passed the House and is now under review in the Senate.[113] If enacted into law, it would require "[a]n analysis of how social media is being used for counter-radicalization and counter-propaganda purposes," regardless of whether such efforts were from the Government or other entities, such as technology companies.[114] This bill is rather significant, because to an everyday citizen and any social media user, knowing that the legislature is holding federal agencies accountable for their endeavors in combating terrorism on the Internet arena restores public faith. It instills confidence in the American people and also provides the legitimate ground in law, for the Government to carry out its counterterrorism agenda more freely, so that it would not necessarily create conflicts as seen in Apple or Twitter's case.

In contrast, the Senate introduced a bill on December 8, 2015 called Requiring Reporting of Online Terrorist Activity Act,[115] whose purposes demand a comprehensive "reporting of terrorist activities and the unlawful distribution of information relating to explosives."[116] The gist of this legislation is to compel electronic communication service providers to immediately provide the Government with the information on terrorism, upon having any "knowledge of any terrorist activity" under the facts or circumstances. The terrorist activity includes those outlined in Section 842(p) of Title 18 of the United States Code,[117] referring to the type of activity that "involves distribution of information relating to explosives, destructive devices, and weapons of mass

---

111 H.R. 3654, 114th Cong. (1st Sess. 2015).
112 H.R. 3654.
113 H.R. 3654.
114 H.R. 3654.
115 S. 2372, 114th Cong. (1st Sess. 2015).
116 S. 2372.
117 18 U.S.C. § 842 (2012).

destruction."[118] The bill does not specify the methods or mechanisms by which technology companies can provide the Government with such information. However, it is safe to assume that such bilateral communication will be transmitted through the Internet. If this bill was enacted into law, all entities that "engaged in providing an electronic communication service or a remote computing service to the public . . . [upon] actual knowledge of any terrorist activity"[119] would be required to produce their knowledge of facts and circumstances to the designated governmental agencies.[120]

This proposed legislation would essentially cover all technology companies and providers of Internet communications. Although the benefits of acquiring such information would be enormous for national security purposes, the costs and burden on the third-party entities would be overbearing as well. Currently still at the introduction stage of the legislative process, as of this writing, it is not clear whether the bill will eventually become law. What can be expected, however, is that tech giants and electronic communication service providers will surely contest the constitutionality of this legislation once it became law, if not lobbying against the bill. For example, in expressing their opposition to this bill, civil liberty activists and human rights groups voiced their criticism of the bill to the Senate Judiciary Committee, contending that the bill contains "several fundamental flaws and would create a significant chilling effect on constitutionally protected speech."[121] Specifically, they oppose that the scrutiny that the bill imposes—by requiring service providers to report "terrorist activity," a potentially overboard category of conduct and speech—"will unavoidably exert a chilling effect on protected speech and will burden individuals' First Amendment rights to speak and to access information."[122]

This criticism is not unfounded. This is because leading technology companies already have existing systems and measures in place, helping to catch and eliminate threats, incitements, and

---

118 S. 2372.

119 S. 2372.

120 S. 2372.

121 *Coalition Letter Opposing S. 2372, The Requiring Reporting Of Online Terrorist Activity Act*, AM. CIV. LIBERTIES UNION (Dec. 16, 2015), https://www.aclu.org/letter/coalition-letter-opposing-s-2372-requiring-reporting-online-terrorist-activity-act.

122 *Id.*

terrorism, out of their own spirits as corporate citizens.[123] For example, Twitter prohibits its users from promoting violence, threats or terrorism and will temporarily lock or permanently suspend violating accounts.[124] Google maintains a similar policy.[125] Facebook, for instance, "prohibits expressions of support for 'dangerous organizations,' and ban '[s]upporting or praising leaders of those same organizations, or condoning their violent activities.'"[126] Therefore, as the critic of the Senate's proposed bill predicts, "mandating affirmative monitoring beyond existing practices would sweep in protected speech and turn the social media companies into a wing of the national security state."[127] The fate of this legislation remains to be seen.

In any event, in the quest of gathering intelligence to serve national security interest, the U.S. Government should engage dialogues with technology companies in a way that would ensure that tech giants are able to meet the needs of their customers, exercise free speech, uphold their corporate values, and provide privacy for the general public. The executive branch should consider delegating a special committee wholly dedicated to channel regular communications with tech giants, exchanging thoughts on the war against on terrorism, brainstorming strategies to combat cyber threats, and reaching an understanding that is mutually beneficial in protecting national security. The legislative branch should continue to work on introducing bills that would meet the executive branch's regulatory demands, without abridging third-party citizens or corporate citizens' rights and interests. The courts, as seen in cases discussed above, will be the ultimate weighing scale that will determine whether national security interest should ever be served at the expense of one's right to privacy, free access to information, or freedom of speech.

---

123 *See* Handeyside, *supra* note 110.

124 *See Twitter Rules,* TWITTER, https://support.twitter.com/articles/18311 (last visited March 21, 2017).

125 *See Terms & Policies*, GOOGLE, https://www.google.com/intl/en_us/+/policy/content.html.

126 Handeyside, *supra* note 110.

127 *Id.*