

Exhibit B

Group, Terrorist Screening Center, and Weapons of Mass Destruction Directorate. The FBI's National Security Branch also guides the functions carried out by other FBI divisions that support the FBI's national security missions, such as training, technology, human resources, and any other operations that further the FBI's mission to defeat national security threats directed against the United States. In this role, I have official supervision over all of the FBI's investigations to deter, detect, and disrupt national security threats to the United States.

3. As the Acting Executive Assistant Director of the National Security Branch, I have also been delegated original classification authority by the Director of the FBI. *See* Executive Order 13526, 75 F.R. 707 (Dec. 29, 2009), Section 1.3 (c). As a result, I am responsible for the protection of classified national security information within the National Security Branch of the FBI and in matters affecting the national security mission of the FBI, including the sources and methods used by the FBI in the collection of national security and criminal information for national security investigations. To that end, the Director of the FBI has authorized me to execute declarations and affidavits to protect such information.

4. I submit this declaration in support of an assertion of the state secrets privilege by the Attorney General in order to protect classified national security information provided to the Court in the Classified Declaration of EAD Michael B. Steinbach ("Classified Steinbach Declaration"). The purpose of the Classified Steinbach Declaration was to describe—in classified detail—the national security harms that reasonably could be expected to result from the disclosure of information that Plaintiff Twitter, Inc., ("Twitter") sought to publish in a draft Transparency Report, which I understand to be the subject of this litigation. I have personally

reviewed the Classified Steinbach Declaration. As discussed herein, the classified material contained in that declaration includes information concerning critical intelligence-gathering activities and capabilities, the disclosure of which reasonably could be expected to cause serious, or, in some cases, exceptionally grave damage to the national security of the United States.

5. The statements in this declaration are based on my personal knowledge, my review and consideration of documents and information made available to me in my official capacity, and on information obtained from Special Agents and other FBI employees. I have reached my stated conclusions in accordance with this information.

II. BACKGROUND

A. National Security Legal Process

6. Several federal statutes authorize the FBI to obtain information from individuals or private entities, including electronic communication service providers (“providers”), in furtherance of investigations conducted to protect the national security of the United States. Under 18 U.S.C. § 2709, 12 U.S.C. § 3414, and 15 U.S.C. §§ 1681u, 1681v, the FBI may issue National Security Letters (“NSLs”). The Foreign Intelligence Surveillance Act (“FISA”) provides different mechanisms for the Government to obtain foreign intelligence information in support of its national security investigations, including: Title I, authorizing electronic surveillance within the United States; Title III, allowing physical searches in the United States; Title IV, permitting the installation of pen registers and trap and trace devices; Title V, for access to certain “tangible things;” and Title VII, permitting the acquisition of foreign intelligence information concerning subjects outside the United States. *See* 50 U.S.C. §§ 1801 *et seq.*

7. This declaration refers at times collectively to NSLs and FISA orders and directives as “national security process” or “national security legal process.” In some circumstances, data reflecting the Government’s use of such process, including qualitative and quantitative information about the national security process received by a particular individual or entity, is classified and subject to nondisclosure requirements imposed by statute or court order or both.

8. I understand that Twitter filed this lawsuit in order to challenge the limitations on its ability to publicly report data reflecting specific numbers and types of national security legal process that Twitter received during the six month period from July 1 through December 31, 2013, and to publish similar data for future timeframes.

B. Provider Reporting Regarding Receipt of National Security Process

9. As EAD Steinbach explained, following unauthorized disclosures by Edward Snowden of documents that purportedly contained classified national security information, multiple providers sought to disclose data regarding their receipt of national security process to correct perceived inaccuracies in the press and to address public speculation about the nature and scope of their cooperation with the Government.

10. Citing exceptional circumstances, including the need to facilitate transparency and the impact of secrecy on providers, in 2014 and 2015, the Director of National Intelligence (“DNI”) declassified certain categories of data reflecting the Government’s use of national security process, to permit disclosure of such data by recipients of national security process if reported in one of a number of specified formats. As noted in EAD Steinbach’s Declaration, the categories of data reflecting the Government’s use of national security process declassified by the DNI in

2015 that providers and others may choose to publicly report are set forth in Section 603 of the USA FREEDOM Act and codified at 18 U.S.C. § 1874.

11. The reporting framework reflected in the 2015 DNI declassification and the USA FREEDOM Act allows providers to report aggregate data regarding their receipt of national security process with more granularity than had ever been permitted before. Under each of the permissible reporting formats recognized by Congress: (1) if a recipient of national security process chooses to publicly report quantitative information revealing that it received *any* national security process, it must report statistics regarding process received in every category of authorities, even if that provider received no process pursuant to a particular category; (2) the allowable methods of reporting are all structured as defined aggregate quantities of national security process, varying in scale depending on defined categories of national security process (“bands”); and (3) each category of reporting bands begins at “0.”

12. As EAD Steinbach explained, the currently-operative reporting framework allows electronic communication service providers and others who are subject to national security process, and the secrecy requirements that accompany such process, latitude to describe the process that they have received without unduly compromising national security interests. Information at a more granular level than described in the USA FREEDOM Act remains classified, because it would provide a roadmap to adversaries revealing the existence of or extent to which Government surveillance may be occurring at Twitter or providers like Twitter.

C. Background Regarding the Classified Steinbach Declaration

13. As stated above, I understand that Twitter filed this lawsuit in order to challenge the

limitations on its ability to publicly report data regarding its receipt of national security process under the above-referenced framework; that Twitter sought to disclose data regarding its receipt of national security process that was far more granular than that which had been declassified by the DNI; and that the Government submitted, *ex parte* and *in camera*, the Classified Steinbach Declaration in order to demonstrate for the Court that the information Twitter seeks to publish is properly classified and the harms to national security that could reasonably be expected to result from disclosure of that information. The classified content of the Classified Steinbach Declaration – the information over which the Attorney General is asserting the state secrets privilege – explains in classified terms why the data Twitter seeks to publish is more granular than permitted by the framework reflected in the USA FREEDOM Act and the DNI declassification, and why disclosure of that data reasonably could be expected to cause significant harm to national security.

14. I also have been informed that counsel for Twitter has made a request to the Court for access to the Classified Steinbach Declaration, and that the Court thereafter issued an Order to Show Cause why the Government should not be compelled to disclose the Classified Steinbach Declaration to Twitter's counsel. I also understand that to facilitate access to this classified document (and potentially other classified information in discovery), the Court previously ordered the Government to initiate a background investigation of Twitter's counsel for purposes of providing counsel with a security clearance.

15. Pursuant to the requirements of Executive Order No. 13526, former EAD Carl Ghattas, a predecessor in this role, reviewed the Classified Steinbach Declaration and, as discussed in

greater detail in Section V, below, determined that, although the background investigation of Twitter's counsel was favorably adjudicated, he does not meet the requirements for access to the classified FBI information at issue in this case on the grounds that counsel does not have a "need-to-know" that information.

16. The Attorney General is asserting the state secrets privilege to protect the Classified Steinbach Declaration from disclosure. The remainder of this declaration supports the Attorney General's assertion of the state secrets privilege in this case by explaining the harms to national security that reasonably could be expected to result from the unauthorized disclosure of the Classified Steinbach Declaration.

III. SUMMARY

17. I have determined that the information described below, contained in paragraphs portion-marked as classified in the Classified Steinbach declaration, is properly classified and that its unauthorized disclosure reasonably could be expected to result in exceptionally grave (Top Secret-marked) or serious (Secret-marked) damage to the national security.

18. In unclassified terms, the classified information contained in the Classified Steinbach declaration, and subject to the Attorney General's state secrets privilege assertion, includes the following four categories of classified information:

- (1) Information regarding national security process that has been served on Twitter;
- (2) Information regarding how adversaries may seek to exploit information reflecting the Government's use of national security process, including disclosures by recipients of any such process;
- (3) Information regarding the Government's investigative and intelligence collection capabilities; and

(4) Information concerning the FBI's investigation of adversaries and awareness of their activities, including sources and methods of investigation and intelligence collection concerning those adversaries.

19. Disclosure of the first category of information at issue – information concerning national security legal process served on Twitter – reasonably could be expected to cause serious damage to national security. Disclosure of specific information concerning the amount and type of national security legal process received by a particular service provider would provide highly valuable insights into where and how the United States is or is not deploying its investigative resources, and would tend to reveal which communications services may or may not be secure, which types of information may or may not have been collected, and thus whether or to what extent the United States is or is not aware of the activities of these adversaries.
20. Disclosure of the next two categories of sensitive information set forth in the Classified Steinbach Declaration – detail regarding how an adversary could exploit provider disclosures regarding receipt of national security process and discussion of the Government's collection capabilities – both reasonably could be expected to cause serious damage to the national security, because they would provide a roadmap for adversaries as to how to exploit to their advantage information concerning Government intelligence collection activities.
21. Disclosure of the fourth category of sensitive information set forth in the Classified Steinbach Declaration, information concerning the FBI's investigation of adversaries and awareness of their activities, including sources and methods of investigation and intelligence collection concerning those adversaries, reasonably could be expected to cause serious, and in

some cases, exceptionally grave, damage to the national security.

22. For these reasons and others explained below and in my classified declaration, information falling within the categories described above is currently and properly classified and subject to the Attorney General's assertion of the state secrets privilege because disclosure reasonably could be expected to cause serious or exceptionally grave damage to the national security of the United States.

IV. HARM OF DISCLOSURE OF PRIVILEGED INFORMATION CONTAINED IN THE CLASSIFIED STEINBACH DECLARATION

A. Information regarding any national security legal process served on Twitter

23. The first category of classified information over which the Attorney General is asserting privilege concerns specific detail regarding any national security legal process that has been served on Twitter. This category of information includes (1) particular information regarding the subject matter of certain FBI national security investigations as well as the communications targeted with national security legal process; and (2) the quantity of any national security legal process that has been served on Twitter—such as the data contained in the draft Transparency Report at issue in this case.

24. The first type of information in this category cannot be described in greater detail in this unclassified setting. But the disclosure of the FBI investigative information at issue in this category reasonably could be expected to cause serious damage to national security.

25. The second type of information in this category at issue includes detail set forth in the Classified Steinbach Declaration regarding the quantity of national security process that Twitter has received (including information contained in Twitter's draft Transparency Report), the

disclosure of which reasonably could be expected to cause significant harm to national security. Data contained in the Classified Steinbach Declaration regarding national security legal process received by Twitter would reveal or tend to reveal information about the extent, scope, and reach of the Government's national security collection capabilities and investigative interests. The disclosure of such information would allow adversaries of the United States, including current and future targets of FBI national security investigations, significant insight into the U.S. Government's counterterrorism and counterintelligence efforts and capabilities, or, significantly, the lack thereof; and into particular intelligence sources and methods.

26. The Director of National Intelligence declassified certain aggregate quantities of data reflecting the Government's use of national security legal process to permit public reporting by recipients of such process, if reported in one of the formats specified by the Government.² Those formats were designed specifically to minimize the harms that could reasonably be expected to result from disclosure of this data if publicly reported as specific quantities and types of process or in smaller aggregate quantities. Granular data regarding the national security legal process received by Twitter, which data is contained in the Classified Steinbach Declaration, would reveal such information as: (i) incremental increases or decreases in collection, which would show whether the Government has a significant presence or investigative focus on a particular platform; (ii) the collection of content or non-content information, which would show whether

² Although DNI James R. Clapper concluded that the declassified aggregate quantities of data were properly classified because disclosure reasonably could be expected to harm national security, he elected to declassify the information in the interests of transparency and the impact of secrecy on providers.

and to what extent the Government is collecting certain types of information on that platform; and (iii) the fact of whether or when the recipient received a particular type of process at all, which may reflect different collection capabilities and focus on that platform, different types of information collected, and locations of FBI targets.

27. More specifically, by detailing the amount of each particular type of process Twitter had received during a particular period, and over time, this data would reveal the extent to which Twitter was or was not a safe channel of communication for our adversaries. It is reasonable to expect that our adversaries will take action based on such information. Even historical data would be alerting to adversaries by tending to reveal collection capabilities and investigative interests.

B. Information regarding how an adversary can exploit provider disclosures regarding receipt of national security legal process

28. The second category of classified information over which the privilege is asserted is information set forth in the Classified Steinbach Declaration that details how adversaries might exploit provider-specific data regarding receipt of national security legal process, both with respect to Twitter and with respect to any other provider. Although some sophisticated adversaries may already have strategies for exploiting this kind of data, disclosure of this category of information would be tantamount to providing adversaries an instruction manual for how they can effectively take steps against the U.S. Intelligence Community.

29. In sum, the information within this category could be used to draw inferences from provider-specific data about the Government's collection efforts and guide adversaries to sophisticated strategies to employ in their activities against the Intelligence Community, and

therefore its disclosure reasonably could be expected to cause serious damage to the national security.

C. The Government's collection capabilities

30. The third category of classified information over which the privilege is asserted is information that would reveal or tend to reveal the Government's collection capabilities. Particularly where there are multiple communication options to choose from and additional services that may come on the market, if adversaries are able to discern the Government's collection capabilities and deduce which platforms are safest for their communications, they can reasonably be expected to leave platforms where the Government has collection capability in favor of the "safe" communications channels, likely resulting in a loss of intelligence. The specific information that falls into this category, and further reasons why its disclosure reasonably could be expected to cause serious damage to national security, are set forth in my classified declaration.

D. Information regarding investigations of adversaries' activities

31. The final category of classified information over which the privilege is asserted by the Attorney General is information revealing specific investigative targets and activities of adversaries of the United States. The particularized descriptions of these targets and activities contained in the Classified Steinbach Declaration reveal not only the Government's awareness of the activity described in each instance, but, more importantly, disclose to adversaries that those activities were subject to Government surveillance. In so doing, such disclosures tend to reveal—and therefore diminish the utility of—the Government's intelligence sources and

methods used to acquire that information. The disclosure of such information reasonably could be expected to cause serious, and, in some cases, exceptionally grave damage to the national security.

32. In particular, the disclosure of the identities of investigative targets would alert those targets to the Government's interest in their activities and cause them to alter their conduct to avoid detection of their future activities, which would seriously impede efforts to gain further intelligence on their activities. Similarly, the disclosure of information that would tend to describe, reveal, confirm or deny the existence or use of sources and methods of surveillance would again enable a subject to evade detection and, more generally, provide insights into how the Government undertakes investigations – and thereby damage future investigations that might rely on similar methods. Either outcome reasonably could be expected to cause serious or exceptionally grave damage to national security by denying the United States access to information crucial to the defense of the United States both at home and abroad.

V. RISK OF HARM FROM DISCLOSURE TO CLEARED COUNSEL

33. As noted above, I have been informed that Twitter has requested that the Classified Steinbach Declaration be disclosed to its counsel. I understand that the Court previously ordered that the Government conduct a background investigation of Plaintiff's counsel in order to make a security clearance "suitability" determination, and that, after a favorable suitability determination was made, the Court entered an Order to Show Cause why the Government should not be compelled to make such a disclosure. The discussion above explains why disclosure of the foregoing categories of classified information, which are contained in the Classified Steinbach

Declaration, reasonably could be expected to cause significant—serious and in some cases exceptional—harm to national security. The remainder of this declaration addresses why counsel for Plaintiff Twitter will not be permitted access to this classified information, over which the Attorney General is asserting the state secrets privilege, even where counsel has undergone a background investigation showing that he is suitable to receive classified information.

34. In sum, and as set forth further below, a determination of trustworthiness alone is insufficient to obtain access to classified information. The Executive Branch agency responsible for the classified information must also consent to the disclosure of the information at issue, through what is called a “need-to-know” determination. The FBI objects to the disclosure of classified information to Plaintiff’s counsel in this case and has determined that counsel lacks the requisite need-to-know. Access to classified information by private counsel in civil lawsuits such as this would significantly expand access to highly sensitive information and the attendant risk of inadvertent, involuntary, or intentional disclosures that could cause serious damage to national security. The lack of a need-to-know determination for obtaining access to classified information is especially significant where Twitter’s counsel has never previously had access to any of the information set forth in the classified declaration. Finally, an assertion of the state secrets privilege by the Attorney General constitutes a judgment at the highest level of the Department of Justice that the classified FBI information at issue should be protected and excluded from the case as a matter of law, and supersedes any administrative determination by lower level officials regarding access to classified information.

35. First, in addition to a favorable suitability determination, the Executive Branch must consent to granting access to particular classified information. Here, Twitter's counsel lacks the required "need-to-know" determination to obtain access to classified information. The Executive Branch has long recognized that a reliable way to mitigate the risk of unauthorized disclosures of sensitive national security information is to limit the number of individuals who have access to it. This principle is incorporated in Executive Order 13526, which states that a person *may* have access to classified information provided that a favorable determination of eligibility for access has been made by an agency head or the agency head's designee; the person has signed an approved nondisclosure agreement; and the person has a need-to-know the information. Executive Order 13526, Sec. 4.1 (a). A need-to-know is expressly defined by the Executive Order as "a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function." Executive Order 13526, § 6.1 (dd). The need-to-know requirement governs access by any person to classified information, including government personnel with the highest levels of clearance.

36. The need-to-know requirement is a critical facet of the protection of classified information because it ensures that classified information is not disseminated beyond the extent to which dissemination is necessary for the Government to carry out its national security functions. Because, as discussed further herein, every additional disclosure increases the risk of unauthorized disclosure, it is important to keep to a minimum the number of people who have

access to classified information. Thus, Executive Order 13526 provides that disclosure is to be permitted if and only if there is an Executive Branch finding that a person's access is necessary to perform or assist in a governmental function. This provision reflects the judgment that any disclosure beyond that which is necessary for the Government to carry out its functions creates an unjustifiable risk to the national security.

37. As discussed above, former EAD Carl Ghattas determined that Twitter's counsel does not have a "need-to-know" the classified FBI information at issue in this case, which includes the classified material contained in the Steinbach declaration, "and all classified information underlying the bases for the government's classification determinations with respect to data concerning the FBI's use of national security process." *See* Aug. 8, 2017 EAD Ghattas Decl. ¶¶ 17–18. EAD Ghattas reached this conclusion pursuant to the directives of Executive Order 13526, on the ground that "it does not serve a governmental function, within the meaning of the Executive Order, to allow plaintiff's counsel access to the classified FBI information at issue in this case to assist in representing the interest of a private plaintiff who has filed this civil suit against the government." Aug. 8, 2017 EAD Ghattas Decl. ¶ 18. Consequently, Twitter's counsel does not meet the requirements for access to the classified information, irrespective of whether the background investigation was favorably adjudicated. *Id.* I agree with EAD Ghattas' determination.

38. This determination is not based on an individualized finding as to the trustworthiness of counsel for Twitter, but on a recognition that any disclosure of classified national security information carries an inherent risk of harm, even if disclosed to persons who have received the

requisite suitability determination. For this reason, even career government employees who have received a suitability determination for access to classified information may not, by virtue of that determination, obtain access to any and all classified information absent a need-to-know particular information in the performance of a governmental function. Counsel for Twitter does not seek access to classified information in order to assist the government in its functions, but to represent a private party in this civil lawsuit. If access to classified information is extended to cleared private counsel for non-government parties in civil litigation, then private parties would have the ability to vastly extend the distribution of classified information outside of the Government on topics of their choice, simply by bringing lawsuits that put such information at issue. The already existing risks of inadvertent, involuntary, or even intentional disclosures by holders of classified information would be substantially compounded in these circumstances. Private attorneys have obligations to non-government clients that may naturally result in pushing the boundaries of what must be protected and what may be permissibly disclosed. Private parties in civil litigation are also likely to have less familiarity with the necessary safeguards to protect classified information, including in conversations with other persons, at court hearings, or in privileged notes and work product on computers to which the Government would have no access. Access by private counsel in civil cases would also create potential non-governmental individuals for foreign adversaries to target in their quest to access classified information.

39. In particular, private counsel stand apart from Government employees granted access to classified information in performing their governmental duties, whose computers or other modes of access can be closely monitored or restricted, and whose mishandling of classified information

can be sanctioned more directly. The Government undertakes significant measures to protect classified and sensitive information from disclosure, including by training its employees how to handle it, utilizing classified computer networks and Sensitive Compartmented Information Facilities (SCIFs) to store it, and mandating periodic background reinvestigations of personnel with access to it. Even with such safeguards in place, it is a constant challenge to protect classified information from inadvertent or intentional unauthorized disclosures. Exposing classified information to private attorneys in cases such as this is among the significant risks that the “need-to-know” standard is designed to protect against.

40. The lack of a need-to-know determination for obtaining access to classified information is especially significant where Twitter’s counsel has never previously had access to any of the information set forth in the Classified Steinbach Declaration. At most, Twitter has some limited information about national security legal process it may have received from the Government, but it does not know (or have any need to know) the background of any investigations at issue or other additional background and level of detail set forth in the Classified Steinbach Declaration. Neither Twitter nor its counsel have the information regarding the national security threats facing the United States from foreign adversaries described in the Classified Steinbach Declaration, nor particular information about Government collection capabilities also described therein, nor the classified analytical assessment set forth in that declaration as to how more granular disclosures about legal process that may – or may not – have been served on particular communication platforms could be exploited by a foreign power, resulting in significant harm to the United States. This kind of highly sensitive national security information, including about

counterterrorism and counterintelligence matters, is strictly controlled even within the FBI and Intelligence Community and is certainly not shared with counsel in private civil lawsuits based solely on a suitability determination. In sum, even limited disclosure of the information at issue to a private plaintiff's counsel would be unprecedented and would risk significant harm to national security.

41. It is also of particular concern to the FBI that information intended solely for an Article III judge would be turned over to private counsel. Control over the disclosure of classified information belongs to the Executive Branch and not to the Judicial Branch. The Executive Branch frequently entrusts Article III judges, confirmed by the Senate, with classified information in order for courts to perform their judicial functions. *See* 28 C.F.R. § 17.46(c). Article III judges frequently obtain classified information for *ex parte, in camera* review at a level of detail entrusted only to persons with a high level of security clearance, such as in the information in the Classified Steinbach Declaration and this classified declaration submitted to support the Attorney General's state secrets privilege assertion. As former EAD Ghattas explained, for district judges to order the disclosure of such highly classified information to private counsel – particularly *after* it has already been submitted solely for *ex parte, in camera* review – would create a severe disincentive for the Government to share highly classified information with courts to begin with, or at the least would cause agencies to reconsider the level of information they would be willing to provide a court *ex parte*. *See* Aug. 8, 2017 EAD Ghattas Decl. ¶ 20.

42. Finally, the Attorney General, as the head of the Department of Justice, is asserting the


state secrets privilege in this case to protect the classified information described above, based on the determination that the particular privileged information at issue should be protected from disclosure and excluded from further proceedings in litigation in order to prevent a significant risk of harm to national security. The Attorney General's action supersedes any determination by a lower level Executive Branch official concerning access to this information in litigation.

VI. CONCLUSION

43. The information set forth in the classified portions of my classified declaration and in the classified portions of the Classified Steinbach Declaration is properly classified and extremely sensitive. The unauthorized disclosure of this information reasonably could be expected to cause either serious or exceptionally grave damage to the national security of the United States. For the reasons explained above and in my classified declaration, the assertion by the Attorney General of the state secrets privilege over this information should be sustained.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: March 15, 2019


Michael C. McGarrity
Acting Executive Assistant Director
National Security Branch
Federal Bureau of Investigation
Washington, D.C.