[redacted]

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE MOTION FOR DECLATORY JUDGMENT OF A FIRST AMENDMENT RIGHT TO PUBLISH AGGREGATE INFORMATION ABOUT FISA ORDERS	Docket No. Misc. 13-03
IN RE MOTION TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS	Docket No. Misc. 13-04
IN RE MOTION FOR DECLARATORY JUDGMENT TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS AND DIRECTIVES	Docket No. Misc. 13-05
IN RE MOTION FOR DECLARATORY JUDGMENT TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS AND DIRECTIVES	Docket No. Misc. 13-06
IN RE MOTION FOR DECLARATORY JUDGMENT TO REPORT AGGREGATED DATA REGARDING FISA ORDERS	Docket No. Misc. 13-07

DECLARATION OF ANDREW G. MCCABE

I, Andrew G. McCabe, hereby declare as follows, pursuant to 28 U.S.C. § 1746:

[redacted]

[redacted]

1. (U) I am the Acting Executive Assistant Director of the National Security Branch of the Federal Bureau of Investigation ("FBI"), United States Department of Justice. This declaration is submitted in connection with the United States' opposition to the motions for declaratory judgment filed by Google Inc. ("Google"), Microsoft Corporation ("Microsoft"), Yahoo! Inc. ("Yahoo"), Facebook, Inc. ("Facebook"), and LinkedIn Corporation ("LinkedIn") (collectively, the "Movants" or the "providers") in the above-captioned proceedings.[1]

2. (U) I entered on duty with the FBI, as a Special Agent, in 1996. Following several assignments, I served as the assistant section chief of the International Terrorist Operations Section One of the FBI's Counterterrorism Division, where I was responsible for the FBI's counterterrorism investigations in the continental United States. In 2008, I was promoted to Assistant Special Agent in Charge of the Washington Field Office's Counterterrorism Division, which included the division's National Capital Response Squad, Rapid Deployment Team, Domestic Terrorism Squad, Cyber-CT Targeting Squad, and the Extraterritorial Investigations Squads. In September 2009, I was named the first director of the FBI's High-Value Interrogation Group. In May 2011, I became the FBI Counterterrorism Division's Deputy Assistant Director overseeing the international terrorism investigation program. In May 2012, I was named Assistant Director of the FBI's Counterterrorism Division. I served as Assistant Director of the

[1] (U) The motions for declaratory judgment filed by each of the Movants are referred to herein individually as the "Google Amended Motion", the "Microsoft Amended Motion", the "Yahoo Motion", the "Facebook Motion", and the "LinkedIn Motion", respectively, and collectively as the "Motions." Dropbox, Inc. ("Dropbox") has filed an amicus curiae brief in support of the Movants.

[redacted]

[redacted]

FBI's Counterterrorism Division until July 2013, when I was named Acting Executive Assistant Director of the FBI's National Security Branch.

3. (U) As the Acting Executive Assistant Director of the FBI's National Security Branch, I am responsible for, among other things, overseeing the national security operations of the FBI's Counterintelligence Division, Counterterrorism Division, Directorate of Intelligence, High-Value Detainee Interrogation Group, Terrorist Screening Center, and Weapons of Mass Destruction Directorate. The FBI's National Security Branch is also accountable for the functions carried out by other FBI divisions that support the FBI's national security mission, such as training, technology, human resources, and security countermeasures. 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 and its interests as well as to protect against foreign clandestine intelligence activities.

4. (U) As the Acting Executive Assistant Director of the National Security Branch, I also have been delegated original classification authority by the Director of the FBI. See Executive Order 12958, as amended by Executive Order 13292, as amended by Executive Order 13526, 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, 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, I have been authorized by the Director of the FBI to execute declarations and affidavits in order to protect such information.

[redacted]

[redacted]

5. (U) I base the statements contained in this declaration upon my personal knowledge, my review and consideration of documents and information available to me in my official capacity, and information obtained from Special Agents and other FBI employees. I have reached my stated conclusions in accordance with this information.

(U) Background

6. (U) Prior to the events leading to this litigation, a limited number of electronic communication service providers, including Google and Microsoft, publicly disclosed the precise number of unclassified criminal information requests that they receive from all sources. These numbers have included, for example, grand jury subpoenas and criminal search warrants, but do not include Foreign Intelligence Surveillance Act ("FISA") orders or National Security Letters ("NSLs").

7. (U) In early 2013, pursuant to an agreement with the FBI, Google and Microsoft began publicly disclosing, separate and apart from their disclosures about criminal process received, annual aggregate figures regarding the number of NSLs that each company received and the number of accounts affected by the NSLs. Specifically, Google and Microsoft were permitted to disclose, and have now disclosed, the following figures: (a) the number of NSLs that they receive annually, in ranges of one thousand (i.e., 0-999, 1000-1999, etc.); and (b) the number of accounts affected by those NSLs, also in ranges of 1000. See http://www.google.com/transparencyreport/userdatarequests/; www.microsoft.com/about/corporatecitizenship/en-us.reporting/transparency (last visited September 27, 2013); see also Attachment A (letters from the FBI to Google and Microsoft

[redacted]

[redacted]

regarding the NSL disclosures). In connection with their discussions with the FBI about the NSL disclosures, both providers indicated that they did not intend to make comparable disclosures about any FISA orders that they receive.[2] At that time, Yahoo and Facebook did not request authority to make these public NSL disclosures nor were they known to be publicly disclosing through any formal company report the extent to which they received criminal process.

8. (U) In June 2013, Edward Snowden, a former National Security Agency contractor, made well-publicized and self-acknowleged leaks regarding government surveillance programs. Following the Snowden leaks, multiple providers, including Google, Microsoft, Yahoo, and Facebook, sought relief from the FBI in order to correct inaccuracies in press reports and to alleviate public speculation about the nature and scope of the providers' cooperation with the U.S. Government. To address this concern, the FBI agreed among other things to allow the providers to report the number of FISA orders received and accounts affected by these orders, on a semiannual basis, but only as part of a single, aggregate number of criminal and national security-related orders that they received from all U.S. governmental entities, including local, state, and federal entities. This agreement was made in consultation with the United States Foreign Intelligence Surveillance Court ("FISC"). The agreement was subject to the following parameters: (i) the numbers of requests received and the number of user accounts for which data was requested would be stated in ranges of 1000 (i.e., 0-999, 1000-1099, etc.); and (ii) the disclosures would not specify or differentiate between the types of process – e.g., a FISA order,

[redacted]

[redacted]

[redacted]

account tasked under Section 702 of FISA, NSL, or criminal subpoena – received. See Attachment B (letters from the FBI to Microsoft, Yahoo, and Facebook regarding this agreement). The FBI agreed to these unprecedented disclosures to enable the providers to demonstrate to their customers that only a tiny fraction of their customers' accounts were subject to legal process of any kind. It was the view of the FBI that the combined disclosure of all legal process received – criminal and national security – would sufficiently mitigate the harm to national security that would follow from a more disaggregated disclosure of national security process. By aggregating all legal process from all levels of government into "one bucket," neither the receipt of FISA orders, nor any significant increase in the number of FISA orders received or accounts affected, would be discernible due to the large volume of criminal legal process that would also be reported.

9. (U) It was part of the "one aggregate bucket" agreement that a provider could not make the disclosures discussed in paragraph eight while also making either the separate NSL disclosures (discussed in paragraph seven) or the separate criminal process disclosures (discussed in paragraph six). Microsoft, Facebook, Apple, Yahoo, and AOL opted for the arrangement permitting them to make the disclosures discussed in paragraph eight: i.e., disclosure, on a semiannual basis, of aggregate numbers, in bands of 1000, of all process from all governmental entities, without specifying or differentiating between the type of process received.[3]

[redacted]

[redacted]

[redacted]

10. (U) As the providers have recognized in their various transparency reports, publicly reporting a combined number of (a) legal process received and (b) potentially affected accounts has allowed and will continue to allow them to explain that only a very small fraction of their users and accounts are affected by legal process of any kind, much less national security process.

[redacted]

12. (U) Microsoft's numbers are to the same effect. Microsoft's 2012 Law Enforcement Requests Report, which was published before the Snowden leaks, stated the

[redacted]

[redacted]

following: "[I]n 2012, Microsoft and Skype received a total of 75,378 law enforcement requests. Those requests potentially impacted 137,424 accounts. While it is not possible to directly compare the number of requests to the number of users affected, it is likely that less than 0.02% of active users were affected." See www.microsoft.com/about/corporatecitizenship/en-us.reporting/transparency (last visited September 27, 2013). That report goes on to say the following: "We know that law enforcement requests impacted approximately 135,000 Microsoft and Skype accounts in 2012. We have many hundreds of millions of accounts for our online and cloud services. To give you a sense of proportion we estimate that less than two one-hundredths of one percent (or 0.02%, to put it another way) were potentially affected by law enforcement requests." Id. Similarly, following the Snowden leaks and after obtaining permission from the FBI, Microsoft publicly released the total number of law enforcement requests (including national security process) it had received for the last six months of 2012 with this statement: "For the six months ended December 31, 2012, Microsoft received between 6,000 and 7,000 criminal and national security warrants, subpoenas and orders affecting between 31,000 and 32,000 consumer accounts from U.S. governmental entities (including local, state and federal). This only impacts a tiny fraction of Microsoft's global customer base." See http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/06/14/microsoft-s-u-s-law-enforcement-and-national-security-requests-for-last-half-of-2012.aspx (June 14, 2013) (last visited September 27, 2013).[4]

[4] (U) On September 27, 2013, Microsoft published a law enforcement requests report for

[redacted]

[redacted]

13. (U) Facebook made a similar statement after publishing data showing that, for the six months ending December 31, 2012, the total number of user-data requests Facebook received from all U.S. governmental entities was between 9,000 and 10,000 and affected between 18,000 and 19,000 accounts: "With more than 1.1 billion monthly active users worldwide, this means that a tiny fraction of one percent of our user accounts were the subject of any kind of U.S. state, local, or federal U.S. government request (including criminal and national security-related requests) in the past six months. We hope this helps put into perspective the numbers involved, and lays to rest some of the hyperbolic and false assertions in some recent press accounts about the frequency and scope of the data requests that we receive." See Press Release, Facebook Releases Data Including All National Security Requests, http://newsroom.fb.com/News/636/Facebook-Releases-Data-Including-All-National-Security-Requests (June 14, 2013) (last visited September 27, 2013).

14. (U) Likewise for Yahoo: In its motion before this Court, Yahoo states that it "provides electronic communications services to hundreds of millions of people and businesses worldwide, including through electronic mail and instant messaging services." Yahoo Motion at 2. Indeed, Yahoo recently stated that it has more than 800 million monthly active users. See http//news.yahoo.com/yahoo-ceo-says-monthly-traffic-surpasses-800-million-220034655-sector.

---

the first six months of 2013. See www.microsoft.com/about/corporatecitizenship/en-us.reporting/transparency (last visited September 27, 2013). This most recent report, which was filed after this litigation was initiated, does not include "any national security orders [Microsoft] might have received." Id. Nevertheless, as Microsoft was able to say in its 2012 report and its June 2013 statement, "this new data shows that across our services only a tiny fraction of accounts, less than 0.01 percent are ever affected by law enforcement requests for customer data."

[redacted]

[redacted]

html (September 11, 2013) (last visited September 27, 2013). In its September 2013 transparency report, Yahoo publicly reported receiving criminal and national security legal process (to the extent any national security legal process was received) from all U.S. governmental entities for only 40,322 accounts. Yahoo thus concluded: "The total number of accounts specified in these government data requests during the reporting period comprised less than one one-hundredth of one percent of Yahoo users worldwide." See Yahoo Transparency Report Overview, http://info.yahoo.com/transparency-report (last visited September 27, 2013).

15. (U) Finally, LinkedIn presents the same statistical point. LinkedIn represents that it has "over 238 million members," and that, as compared to other providers, it receives "relatively low numbers of requests for member data." LinkedIn Motion at 1; http://press.linkedin.com/Content/Detail.aspx?ReleaseID=313&NewsAreaID=2&ClientID=1 (September 17, 2013) (last visited September 27, 2013). If it accepted the Government's offer to report its total number of criminal and national security orders, LinkedIn could thus presumably advise its users that only a very small fraction of its accounts is affected by legal requests, including national security requests.[5]

[5] (U) Amicus Dropbox has approximately 175 million users. Like the Movants, if it accepted the Government's "one bucket" approach, it would similarly report that only a tiny fraction of its users are affected by any legal process. See Dropbox Amicus Brief, at 2-3; http://techcrunch.com/2013/07/09/dropbox-dbx-conference (July 9, 2013) (last visited September 27, 2013).

[redacted]

[redacted]

(U) The Pending Motions and the Purpose Of This Declaration

16. (U) In their initial Motions filed on June 19, 2013, Google and Microsoft asked the FISC to authorize them to disclose aggregate statistics about orders and/or directives that they have received under FISA, including the provisions of the FISA Amendments Act. Specifically, in their initial Motions, Google and Microsoft sought authorization to disclose two categories of aggregate figures: (a) the total number of FISA orders, if any, that they have received; and (b) the total number of users or accounts encompassed within, or affected by, any such FISA orders. In Google's initial Motion, Google asserted that it would report the numbers in items (a) and (b) in ranges of 1000, starting with zero: i.e., 0-999, 1000-1999, and so on. In its initial Motion, Microsoft did not state how it would disclose the information in categories (a) and (b), i.e., it was not clear whether Microsoft was seeking to disclose FISA information using precise numbers or in ranges.

17. (U) Subsequent to Google and Microsoft filing the Motions described in the preceding paragraph, on August 29, 2013, Director of National Intelligence (DNI) James R. Clapper announced in a public statement on behalf of the Intelligence Community, including the FBI, that he was directing the annual disclosure of national aggregate FISA data, but, critically, not broken down by company receiving such process. Under the DNI's announcement, the Government will release "the total number of orders issued during the prior twelve-month period, and the number of targets affected by these orders." See http://icontherecord.tumblr.com/ (last visited September 27, 2013). As noted, the Government's reporting will not be broken down by company. The disclosed numbers will be reported for each of the following categories of national

[redacted]

[redacted]

security authorities: (i) FISA orders based on probable cause (Titles I and III of FISA, and sections 703 and 704); (ii) Section 702 of FISA; (iii) FISA Business Records (Title V of FISA); (iv) FISA Pen Register/Trap and Trace (Title IV of FISA); and (v) National Security Letters issued pursuant to 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709. In announcing the release of this information, the DNI emphasized that this initiative was consistent with the President's directive to "make public as much information as possible about certain sensitive U.S. Government surveillance programs while being mindful of the need to protect sensitive classified intelligence and national security." See http://icontherecord.tumblr.com/page/2 (August 29, 2013) (last visited September 27, 2013).

18. (U) Thus, combined with the "one aggregate bucket" disclosures that are broken out by company, the public will have full visibility into the numbers and types of process utilized per year (and accounts affected), and companies and their customers will know the full scope, on an aggregate basis, every 6 months as to the percentage of accounts affected at a company. Notwithstanding the U.S. Government's plans to make public an unprecedented amount of national aggregate information concerning U.S. Government surveillance programs, Google and Microsoft amended their initial motions and now seek significantly broader relief than what they had first requested. Whereas Google's initial motion sought declaratory relief that would permit it to publish two data points within ranges of 1000, Google's amended motion seeks declaratory relief that would permit it to disclose eight data points regarding classified FISA process, and to do so in precise numbers rather than bands of one thousand. See Amended Google Motion at 7. Microsoft's amended motion seeks permission to make even more granular disclosures. See

[redacted]

[redacted]

Amended Microsoft Motion at 5. Microsoft seeks permission to release separate statistics "for *each provision of FISA and/or the [FISA Amendments Act]* pursuant to which Microsoft may receive process,"[6] including both the precise number of orders or directives (if any) and the number of accounts affected for each statutory provision. Microsoft also seeks permission to split those numbers further into separate categories for "non-content" requests and "content *and* non-content" requests. *Id.* (emphasis in original).

19. (U) Yahoo, Facebook, and LinkedIn's requests "involve similar, but not identical, requests for relief [as those] filed by Google and Microsoft." Yahoo Motion at 9 n.6; Facebook Motion at 7 n.3. Like Google and Microsoft, these companies also seek declaratory judgments that would permit them to disclose data regarding both the specific number of classified FISA process that they receive, and the particular FISA authorities under which they receive that process. *See* Yahoo Motion at 4; Facebook Motion at 3; LinkedIn Motion at 6.

20. (U) As explained below, the FISA data that Google and Microsoft sought to publish in their initial Motions constitutes information classified at the Secret level because its disclosure could reasonably be expected to cause serious damage to the national security of the United States. See Executive Order 13526 § 1.2(a)(2). The harm to the national security is even greater with respect to the significantly more expansive disclosures now sought by the five companies here. This declaration addresses: (1) factors considered by the FBI when classifying information, (2) specific policies that govern the FBI's classification of information, (3) a discussion of how the

[6] (U) If "provision" is interpreted to mean "title" then there would be five "provisions," as five titles of FISA contain information collection authority (Titles I, III, IV, V, and VII). However, if the term "provision" is interpreted to mean "section," the number would be higher.

[redacted]

[redacted]

information sought to be disclosed by the providers would harm national security, and (4) a discussion of how the more detailed and more disaggregated disclosures now proposed by the Movants are even more detrimental to national security than the disclosures initially sought by Google and Microsoft as part of their initial Motions.

21. (U) Each paragraph in this declaration is marked immediately after the number of the paragraph with letters in parentheses, indicating the level of classification and restrictions on dissemination applicable to that particular paragraph. Paragraphs marked with a "U" are unclassified. Paragraphs marked with a "TS" are classified Top Secret. Paragraphs marked with an "S" are classified as Secret. A designation of SI reflects "Special Intelligence" protected as Sensitive Compartmented Information. Designations of "NF" or "NOFORN" reflect information that may not be disseminated to foreign countries or nationals. The "FISA" dissemination control marking denotes that information was obtained or derived from surveillance authorized pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended. The designation "FOUO" refers to information that is for official use only. Because this declaration is itself a classified document, it is being made available to the Court *ex parte*, *in camera*.

(U) Classification of Information

22. (U) The conduct of national security investigations, and the collection, production, and dissemination of intelligence to support counterterrorism, counterintelligence, and other U.S. national security objectives, requires the FBI to collect, analyze, and disseminate information eligible for classification under Executive Order 13526.

[redacted]

[redacted]

23. (U) The decision whether to classify or declassify information, including but not limited to whether the FBI has conducted or is conducting an investigation, the amount and nature of intelligence that the FBI may have collected during an investigation, and how that intelligence was collected, is based on a variety of factors and considerations that are weighed by officials, such as myself, who have been delegated original classification authority. In weighing these factors, some of which are subtle and complex, I assess whether the disclosure of information, at any given time, may lead to an unacceptable risk of compromising the FBI's past or ongoing intelligence gathering efforts with respect to a particular investigation or investigations, and whether disclosure may lead to an unacceptable risk of compromising investigative sources, methods, or techniques. Among other things, my assessment and judgment as to the harm to the national security that reasonably could be expected from disclosure in any given case at any particular time is affected by whether a mosaic of information can be pieced together by our adversaries, both individuals and groups, which would allow them to better evade ongoing investigations and more easily formulate or revise their counter-surveillance efforts.

(U) The FBI National Security Information Classification Guide

24. (U) The Federal Bureau of Investigation National Security Information Classification Guide ("NSICG") provides guidance concerning the classification and level of protection afforded to FBI-originated national security information. The NSICG is issued under authority of Executive Order 13526; Information Security Oversight Office Directive Number 1 (32 CFR Section 2001.10); Department of Justice Security Program Operating Manual; the FBI

[redacted]

[redacted]

Security Policy Manual; and the designated Original Classification Authority of the Executive Assistant Director, National Security Branch.

25. (U) The NSICG identifies categories of information frequently obtained in the course of national security investigations and intelligence analysis and provides guidance on whether information in these categories should be designated Unclassified (U), Confidential (C), Secret (S), or Top Secret (TS).

27. (U) The FISA order information sought to be disclosed implicates the NSICG categories referenced in the preceding paragraph, and accordingly is classified as Secret. The FISA information at issue would provide international terrorists, terrorist organizations, foreign intelligence services, cyber intruders, and other persons or entities who pose a threat to the national

[redacted]

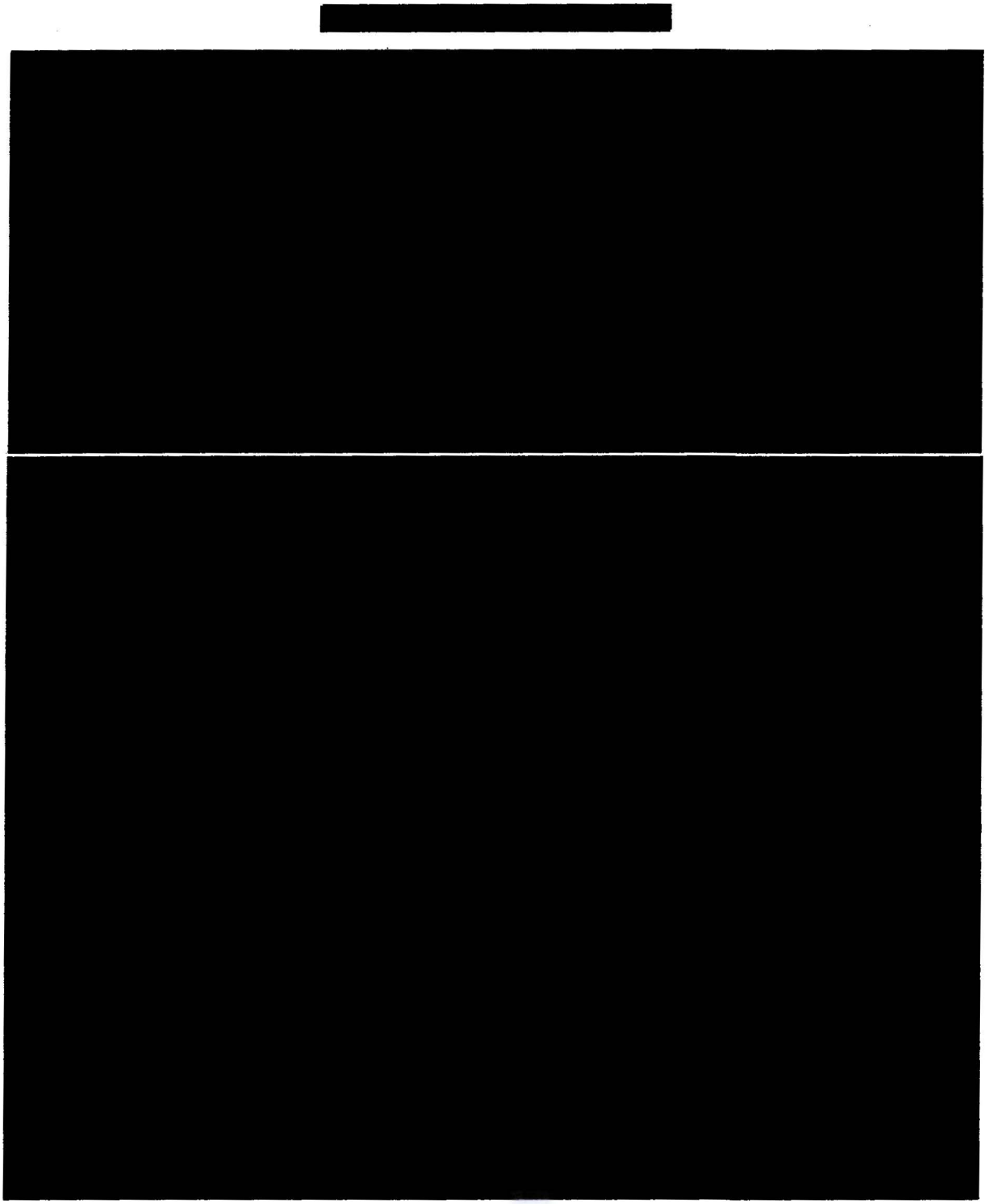
[redacted]

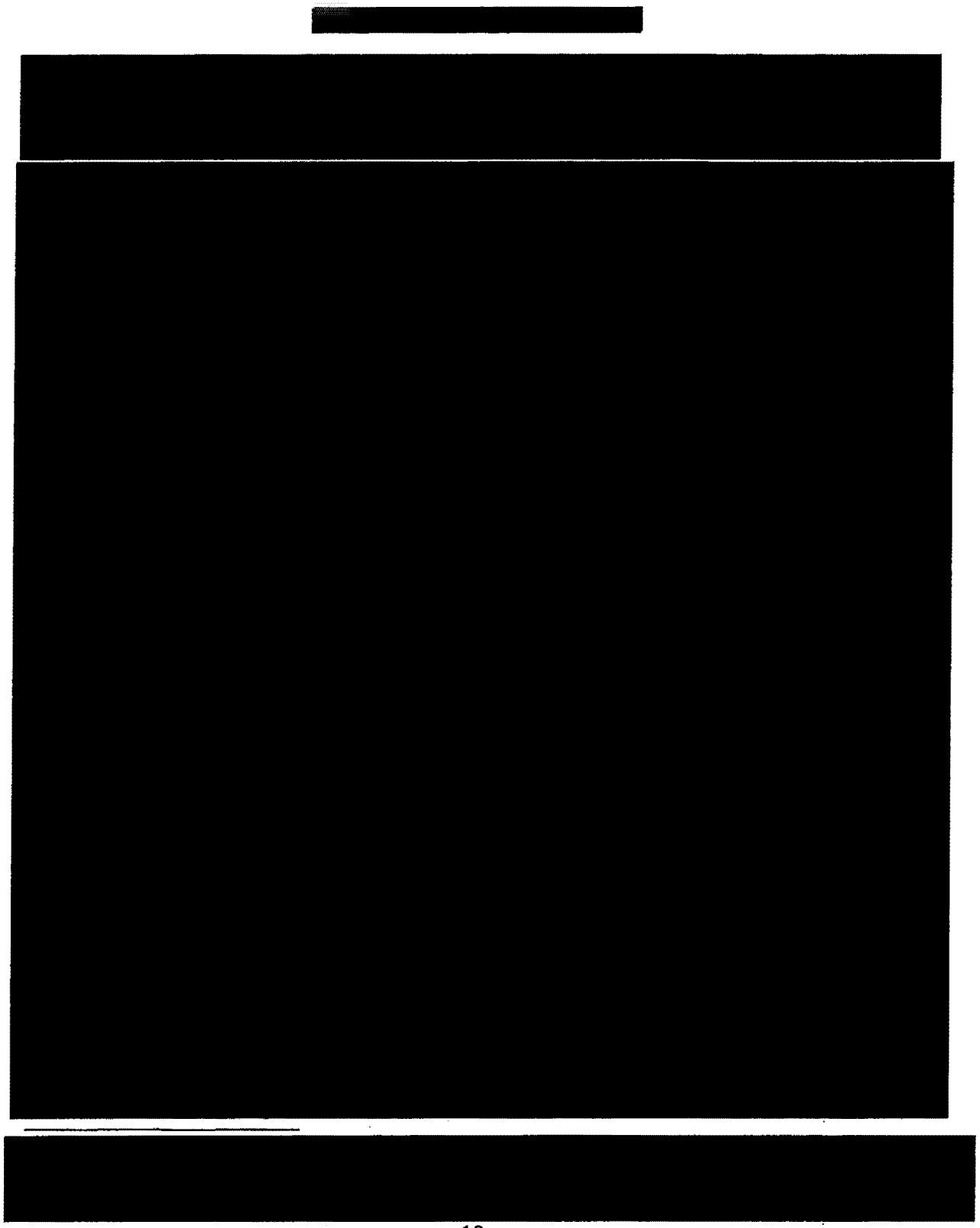
security (collectively, "adversaries") with significant insight into, and information about, the U.S. Government's counterterrorism and counterintelligence efforts and capabilities including, among other things, the Government's collection capabilities under FISA. Armed with this information, adversaries can take action to conceal their activities, alter their methods of operation, or otherwise counter, thwart, or frustrate the ability of the FBI to pursue them. This would undermine both current and future efforts by the FBI to collect foreign intelligence and to detect, obtain information about, or prevent or protect against threats to the national security.

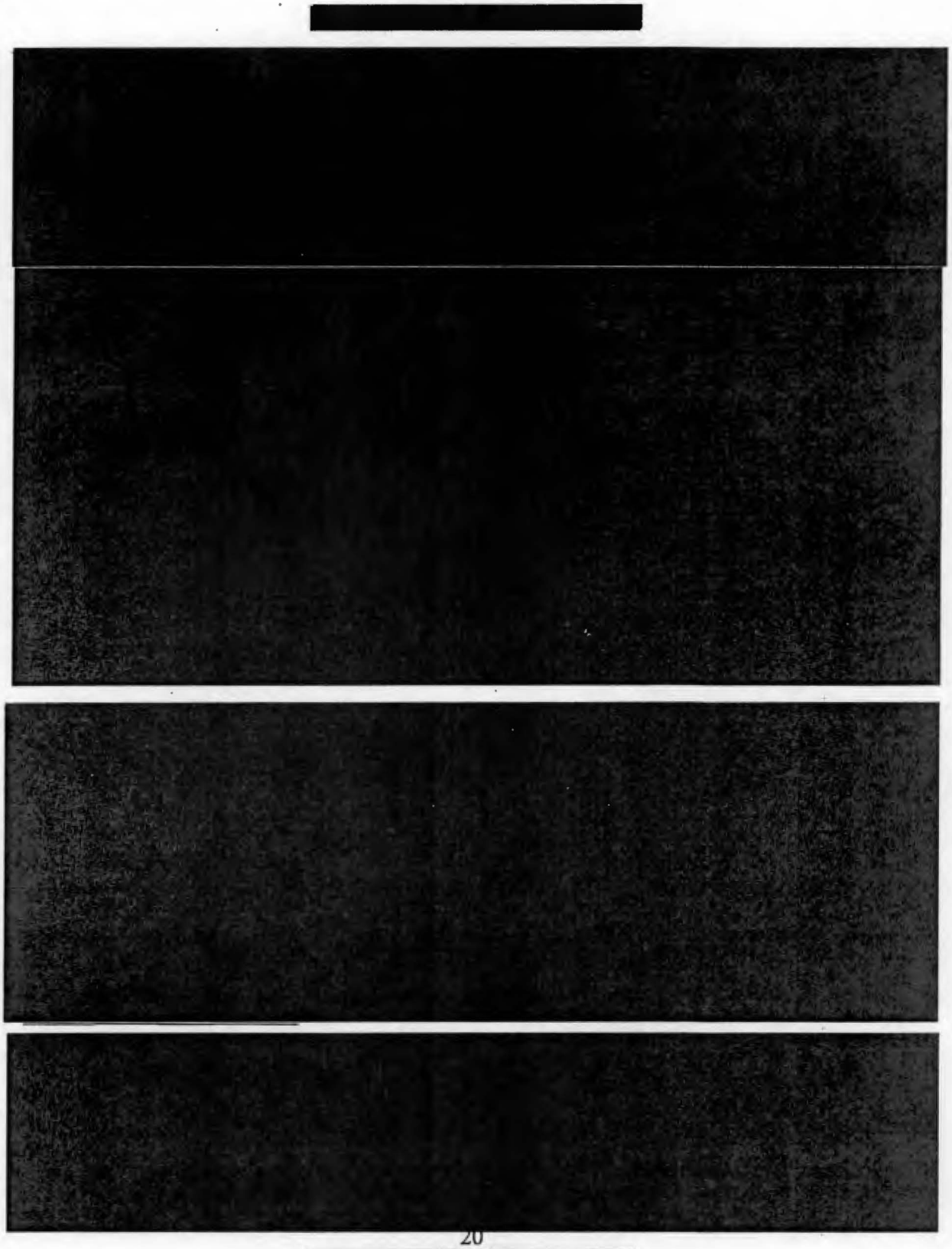
28. (U) National security investigations present evolving challenges, and the FBI's efforts to combat threats to the national security are fluid. The kinds of disclosures requested even in the initial Google and Microsoft Motions have never previously been made. This is all the more true with respect to the more detailed and more disaggregated disclosures now proposed in the current motions by five companies. It would be impossible to specifically identify each and every harm that could arise from the disclosures that the Movants seek to make. However, I note here some of the harms to the national security interests of the United States that would logically flow from the proposed disclosures.

[redacted]

[redacted]







[redacted]

[redacted]

[redacted]

[redacted]

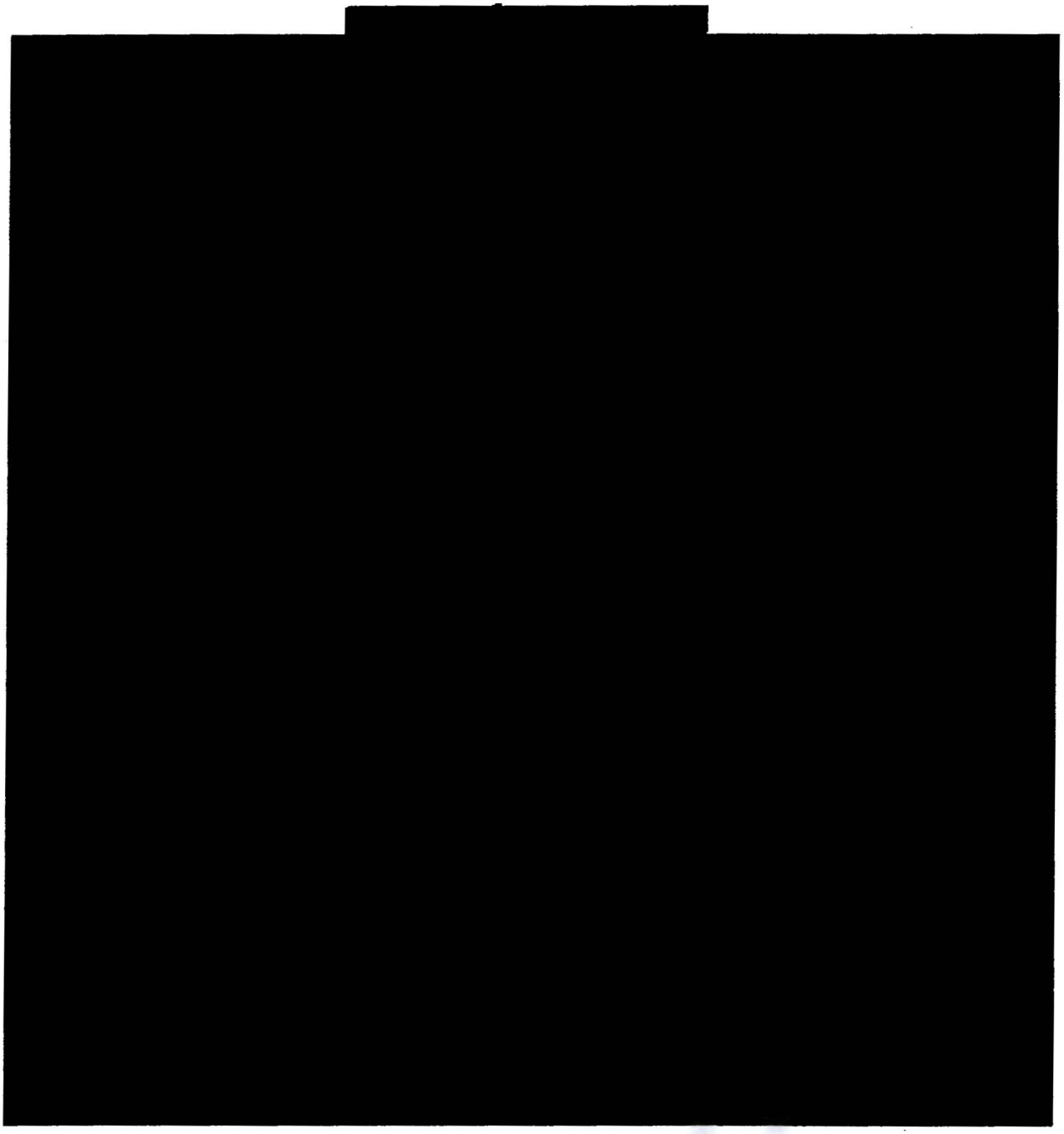
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

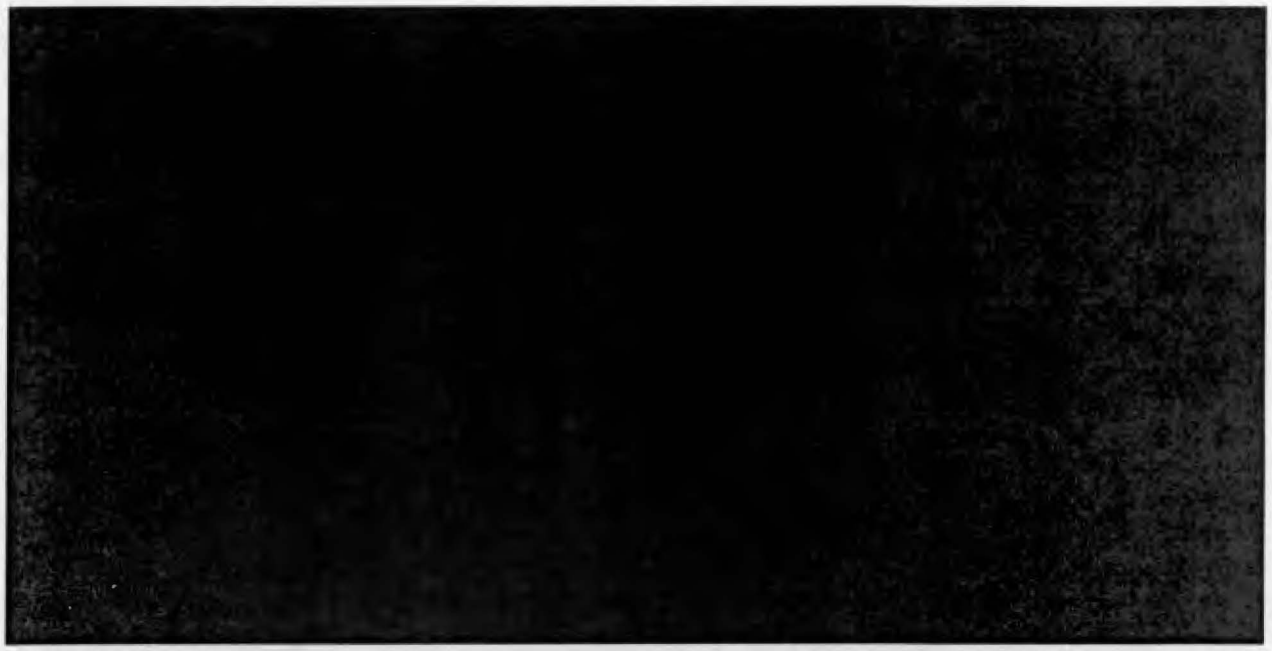


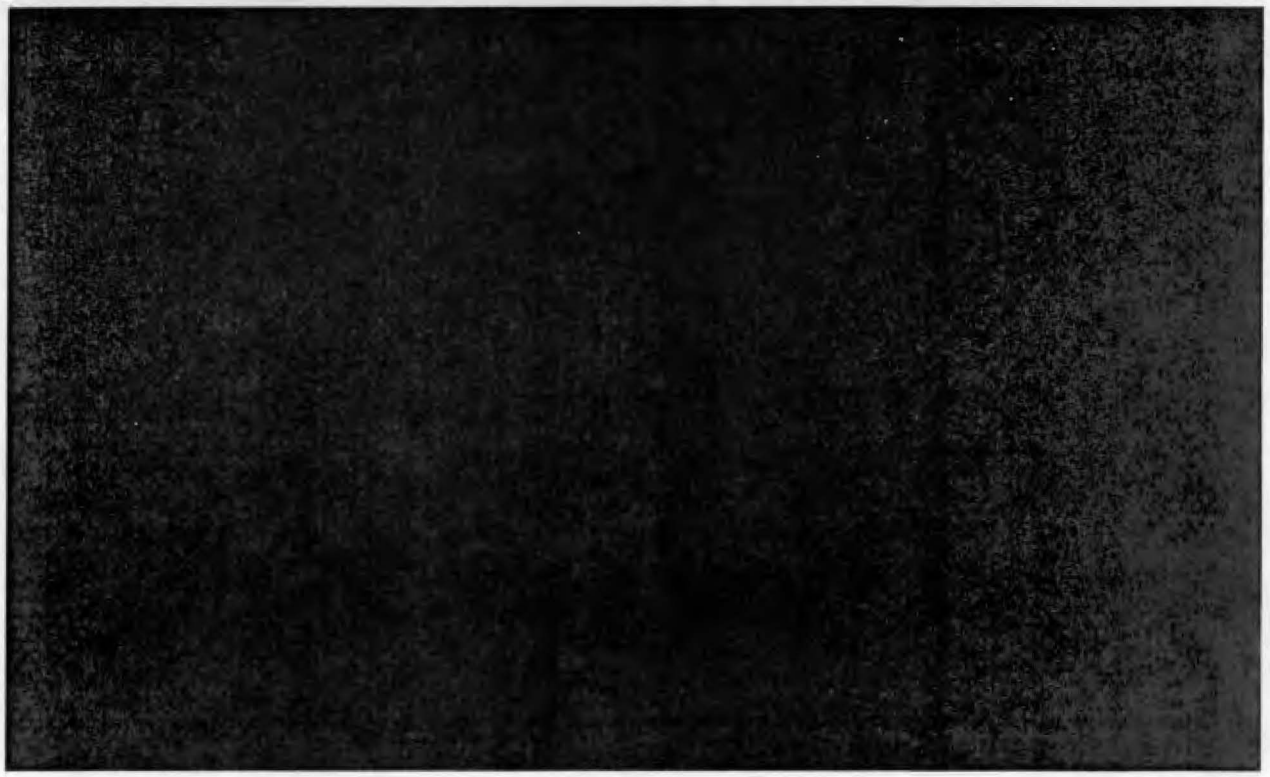
[redacted]

[redacted]

[redacted]

[redacted]





[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

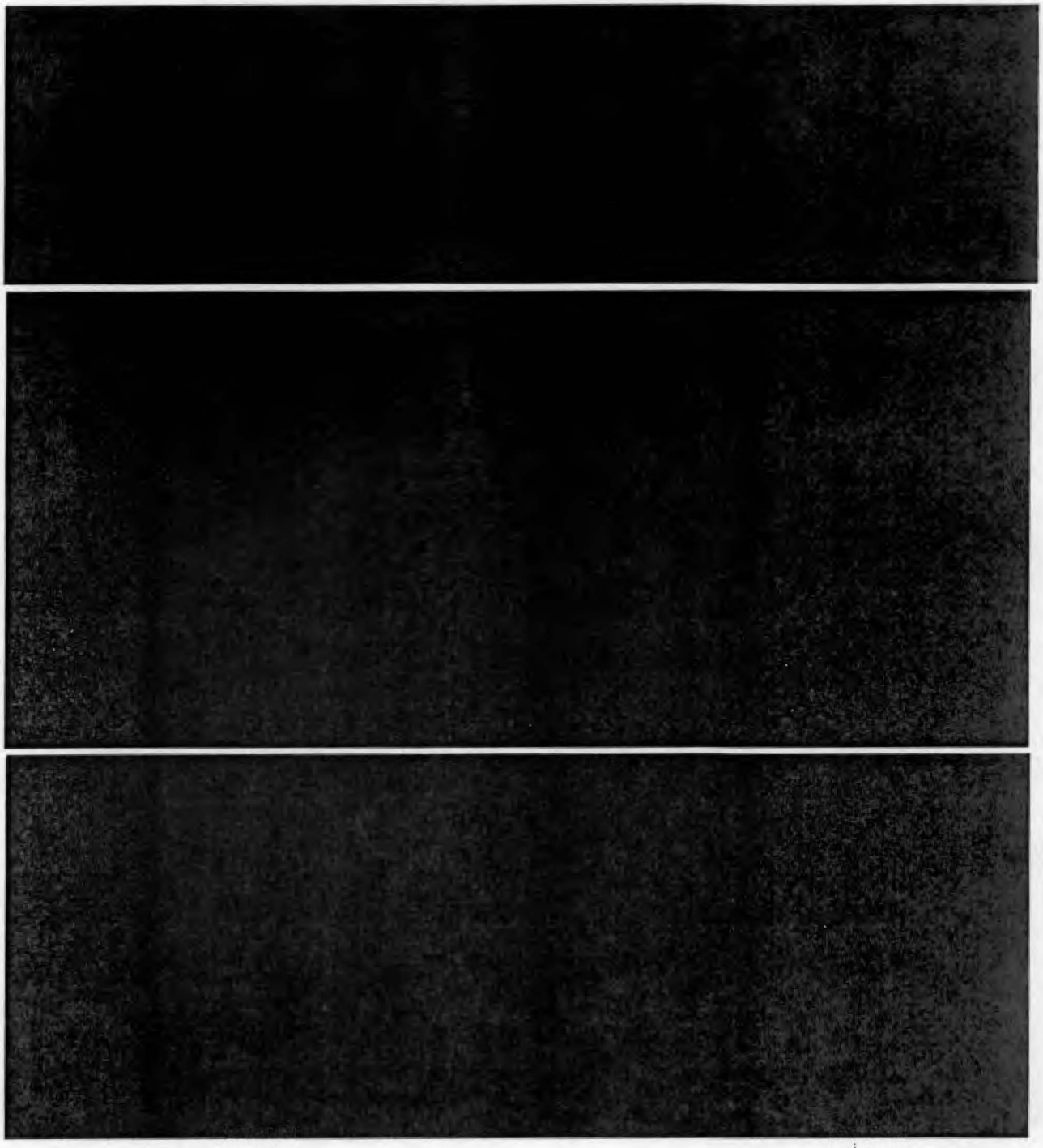
[redacted]

39. (U) Armed with information about the Government's collection capabilities, adversaries will take actions detrimental to the national security. Adversaries may alter their behavior by switching to services that the Government is not intercepting. Should an adversary switch to such services, then the Government would not have an interception or monitoring capability with regard to communications made on these services. This significantly and irreparably undermines current and future counterterrorism and counterintelligence efforts.

[redacted]

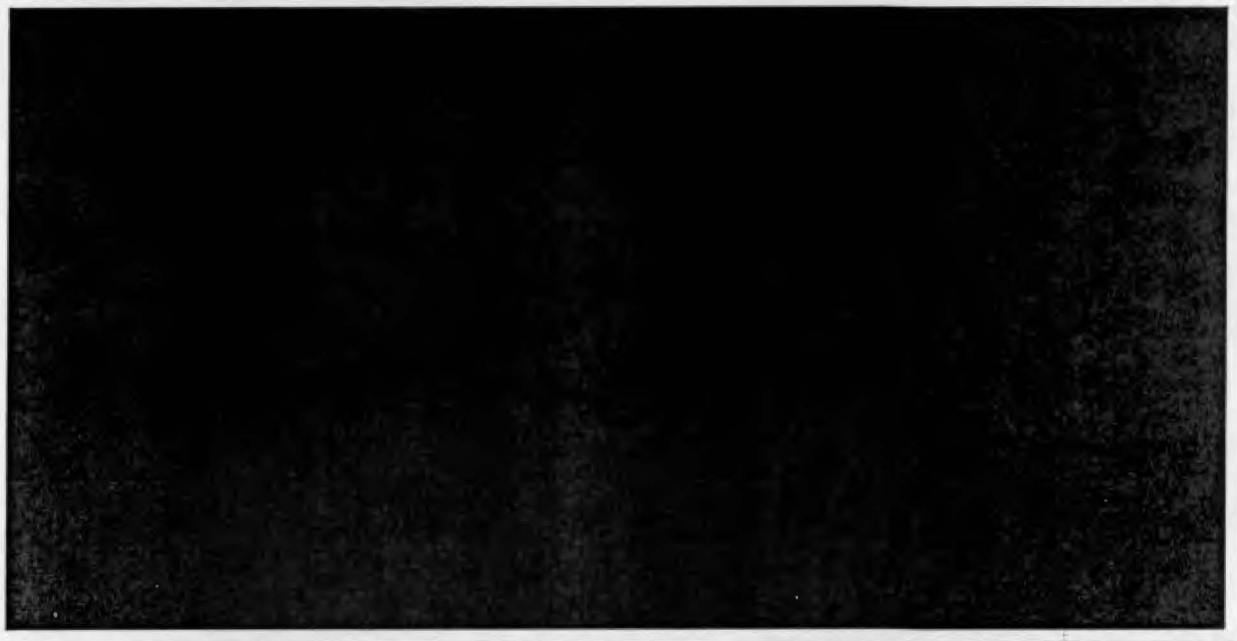
[redacted]

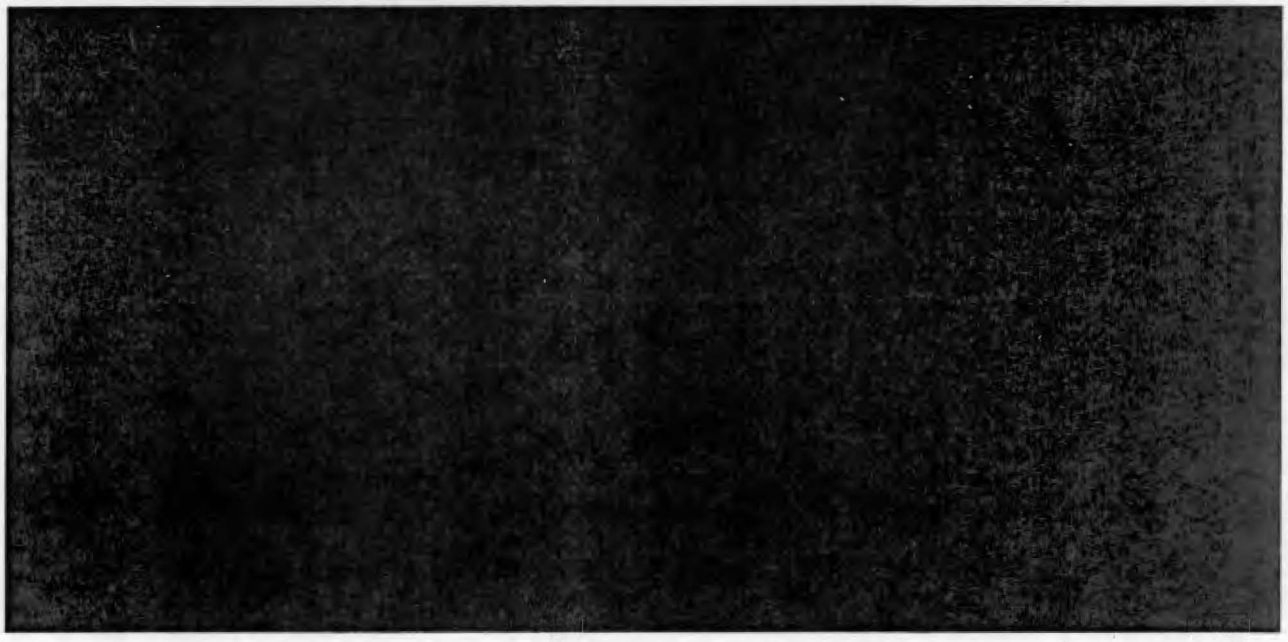
[redacted]



[redacted]

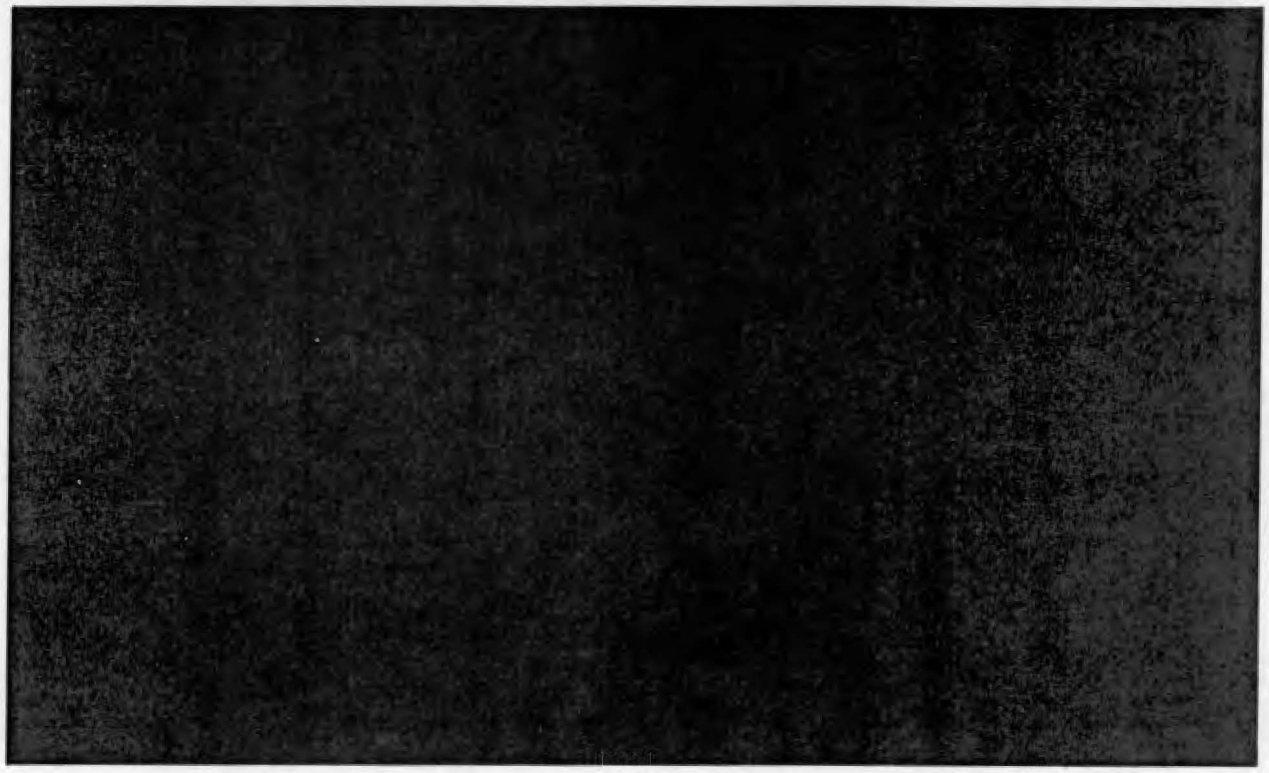
[redacted]





[redacted]

[redacted]



[redacted]

[redacted]

[redacted]

(U) **The Harms to the National Security Will be Compounded By Other Companies Likely Seeking the Same Relief**

48. (U) If Google, Microsoft, Yahoo, Facebook, and LinkedIn are permitted to disclose the FISA information that is the subject of their Motions, it is likely that other companies will seek the same relief. Indeed, initially only Google and Microsoft sought authority from the FISC to disclose publicly the FISA information, and the relief they sought did not include publishing specific numbers or distinguishing among the type of statutory authority used. Barely one month later, Yahoo, Facebook, and LinkedIn have petitioned this Court for authority to disclose their own receipt of FISA orders, and Google and Microsoft have since amended their Motions to publicly

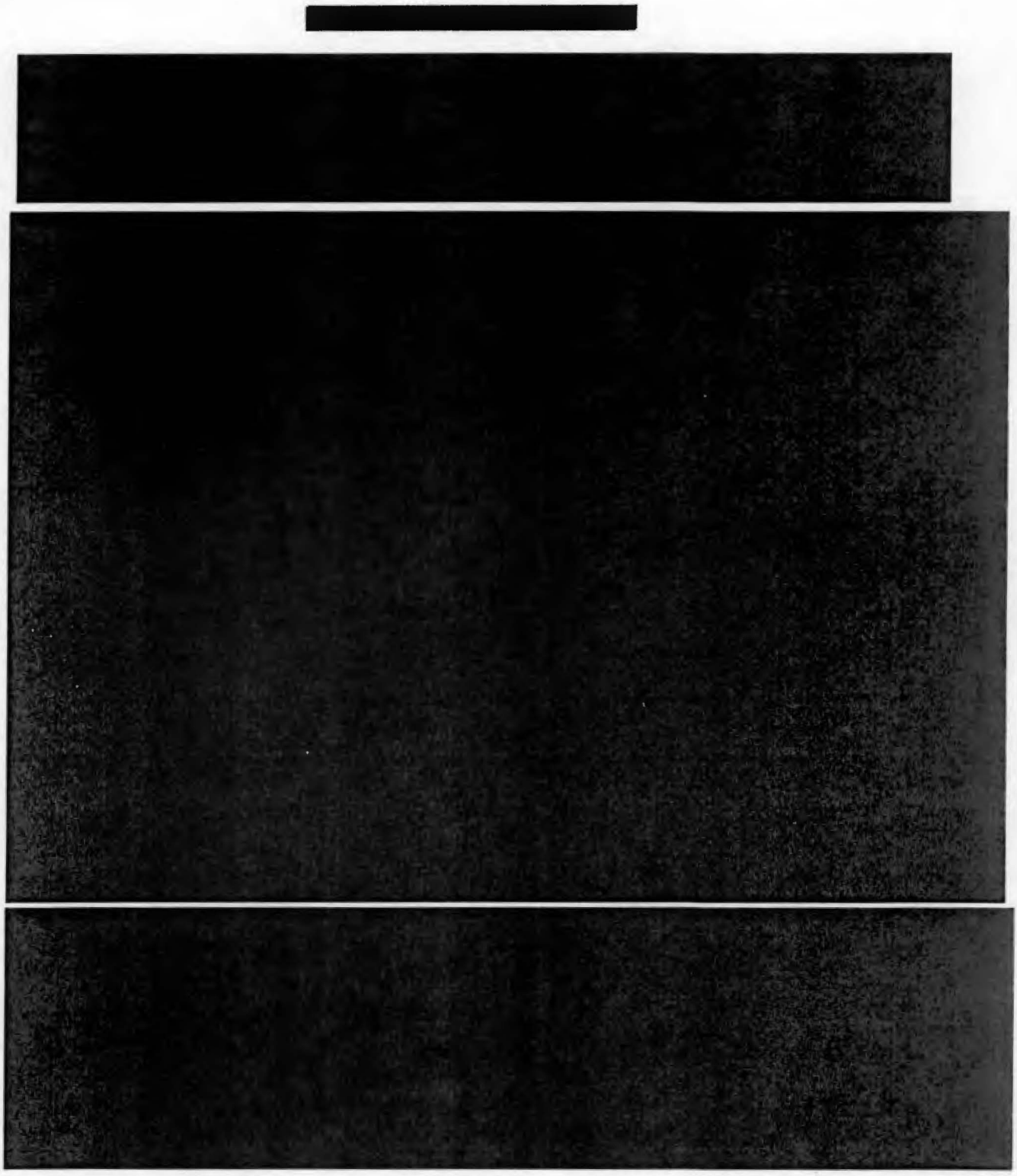
[redacted]

[redacted]

disclose information that is substantially more granular in nature – and thus more revealing of USIC intelligence collection capabilities.

[redacted]

[redacted]



[redacted]

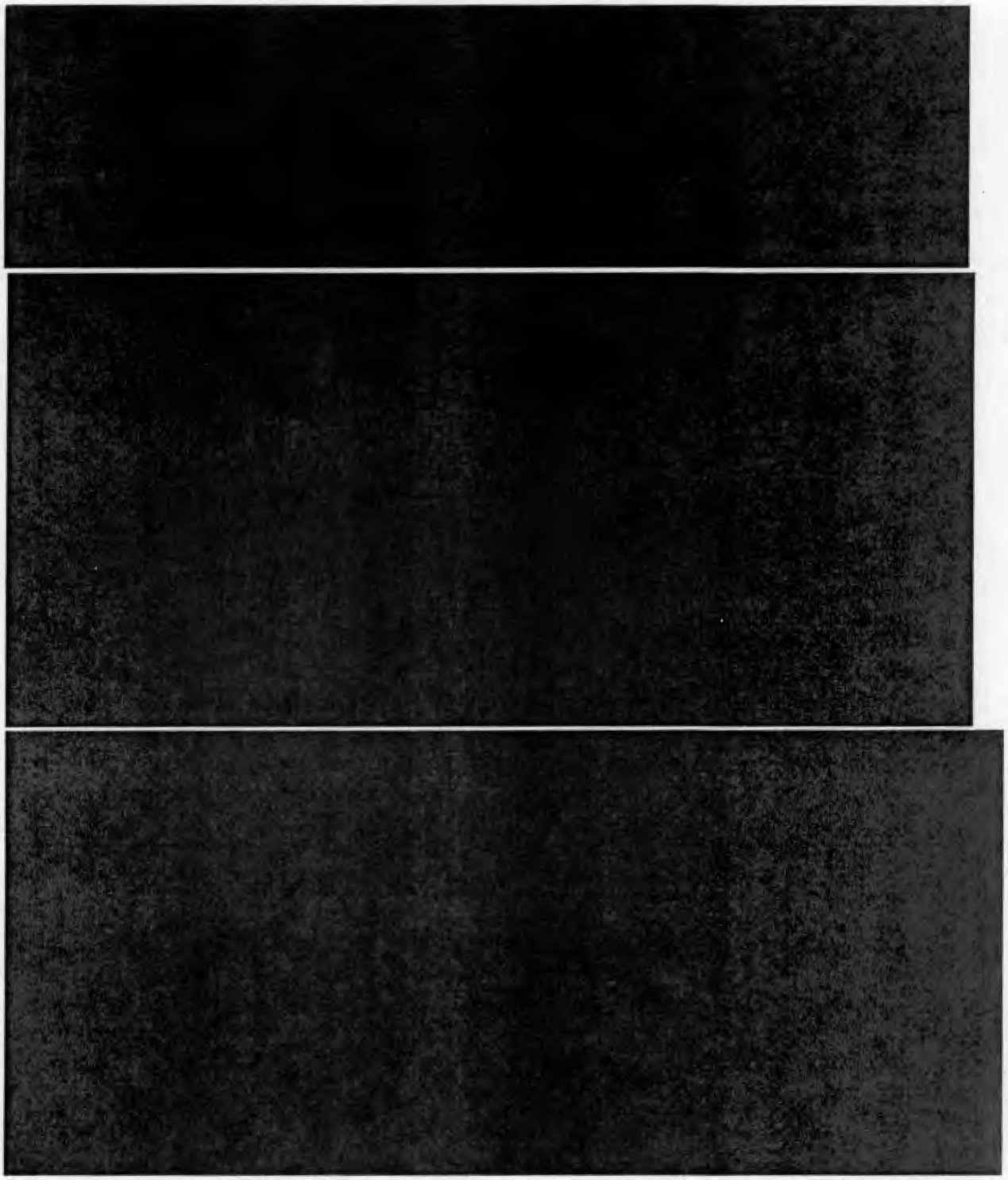
[redacted]

[redacted]

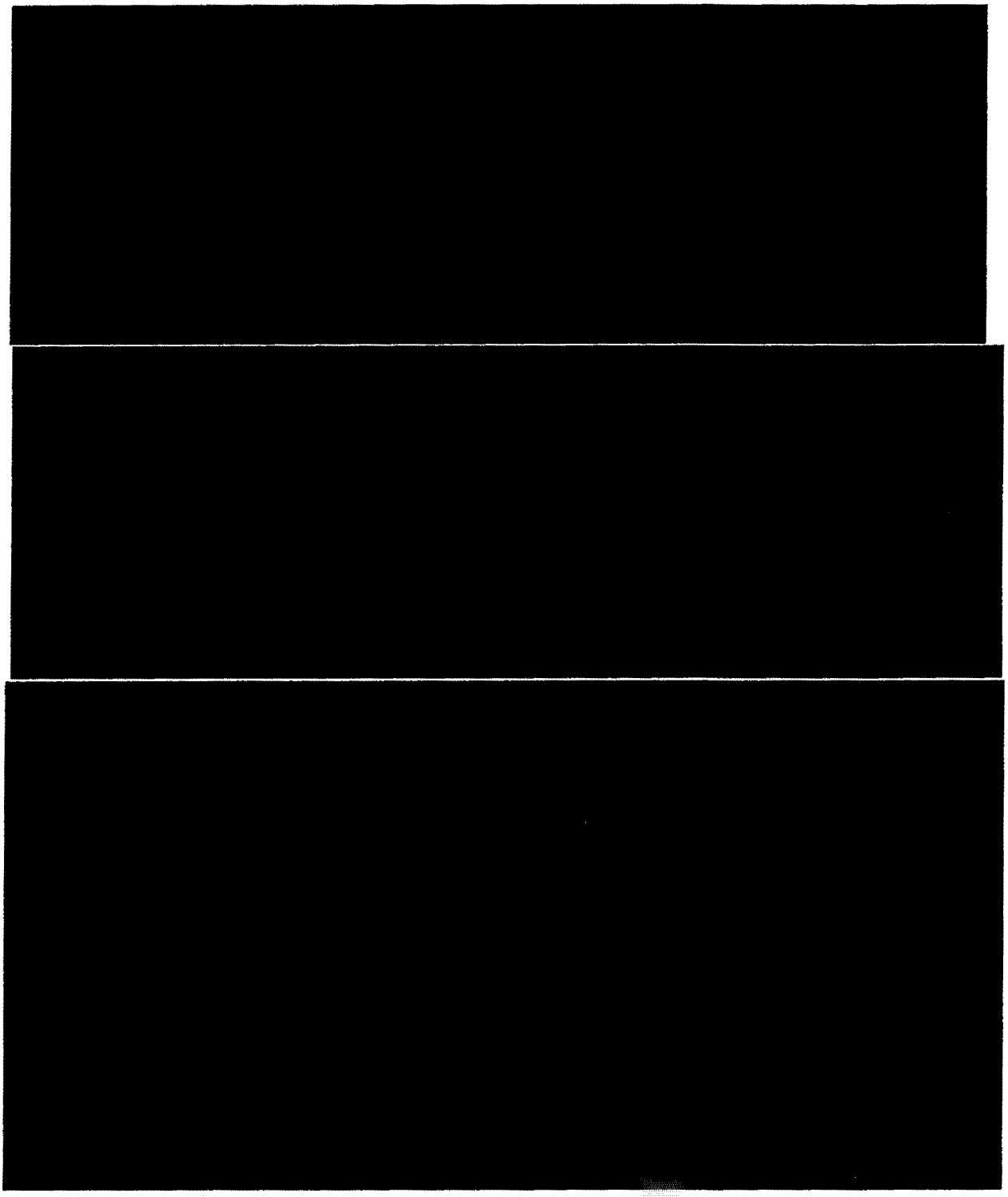
[redacted]

[redacted]

[redacted]



[redacted]



[redacted]

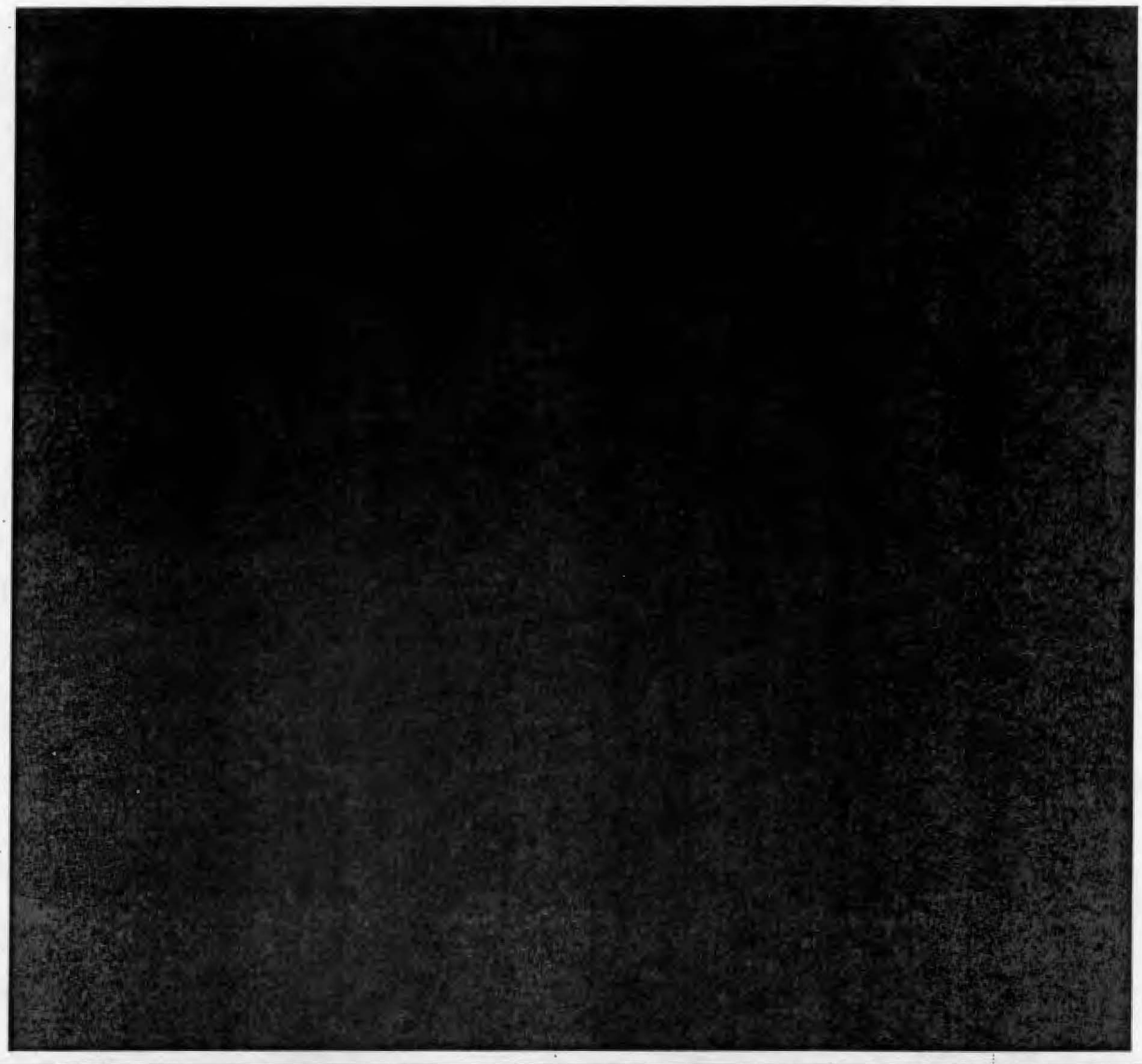
[redacted]

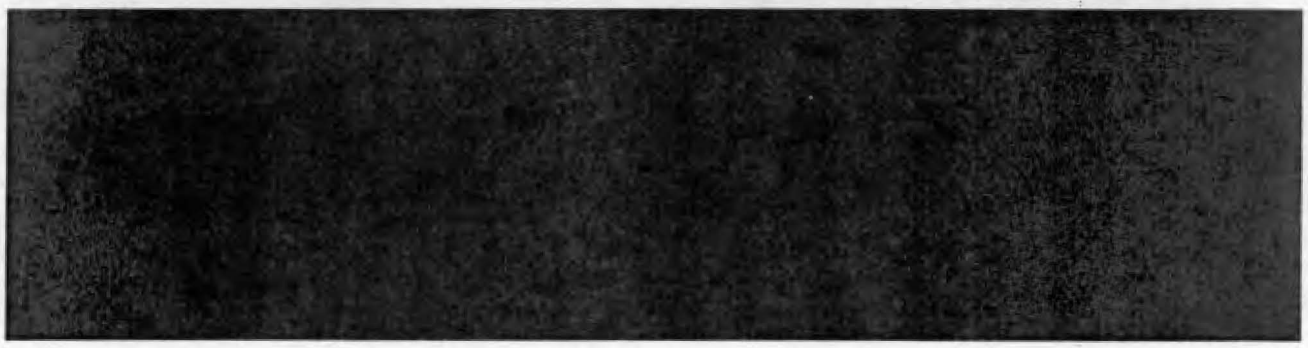
(U) **Prior Disclosures Regarding Receipt of Criminal Process and NSLs Do Not Lead To The Same Harms**

[redacted]

[redacted]

[redacted]





[redacted]

[redacted]

[redacted]

[redacted]

65. (U) Another important distinction is that NSLs are unclassified legal process, whereas FISA orders are classified, generally at the Secret level. The FBI has confirmed that

[redacted]

[redacted]

[redacted]

employees from each of the Movants who work with the FBI on FISA matters have signed binding "Classified Information Nondisclosure Agreement(s)" (SF-312) reflecting their obligation to protect classified information. The current version of the SF-312 nondisclosure agreement went into effect in July 2013. Both the current and prior versions of the SF-312 nondisclosure agreement include the following language: "I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency . . ." See SF-312 Classified Information Nondisclosure Agreement (effective July 2013), available at: http://www.gsa.gov/portal/forms/download/116218; SF-312 Classified Information Nondisclosure Agreement (pre-July 2013), available at: http://armypubs.army.mil/eforms/pdf/S312.PDF.[16] The protection of classified information surrounding FISA orders is of a paramount concern to the United States government. NSLs, which are not classified, present different concerns.

(U) Disclosure of National Aggregate Figures Does Not Give Rise to the Same Concerns

[redacted]

[redacted]

[redacted]

[redacted]

(U) **Conclusion**

67. (U) Protecting the national security of the United States requires that intelligence sources, methods, and techniques be protected from disclosure. In keeping with the above-referenced authorities and after a considered assessment of all of the facts and circumstances concerning this matter, I have concluded that the disclosure of the FISA information at issue in this litigation reasonably could be expected to harm the national security of the United States.

[redacted]

[redacted]

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

Dated: September 30, 2013

Andrew G. McCabe
Acting Executive Assistant Director
National Security Branch
Federal Bureau of Investigation
Washington, D.C.

[redacted]

(U) ATTACHMENT "A"

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

January 29, 2013

Richard Salgado
Director, Law Enforcement and Information Security
Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Re: Disclosure of Limited Information About National Security Letters

Dear Mr. Salgado:

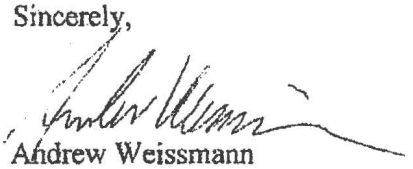
We appreciate your discussions with us over the past few months about your proposal to disclose certain information about the volume of national security letters Google receives from the FBI.

We do not intend to seek to enforce the non-disclosure provisions of the national security letter statute with respect to the proposed disclosures outlined in your letter dated January 15, 2013 (the "Letter"). This position is an exercise of FBI discretion in light of current circumstances and the precise contours of your Letter. Accordingly, our decision does not reflect the FBI's position with respect to potential disclosures by Google that differ in any respect from the disclosures outlined in your Letter. Nor is our decision a precedent for disclosures by any other company that is in receipt of national security letters from the FBI, even if the disclosures were made in the manner that you have proposed in your Letter. The national security implications of disclosures related to the receipt of national security letters may vary depending on the identity of the company that is making the disclosure and the overall number of disclosures by different companies. For this reason, if other companies also seek to disclose information about the volume of national security letters that they receive, that may alter our calculus about the implications of disclosures by Google. In addition, our current determination is based on our prediction about the potential national security consequences of the disclosures outlined in your letter. We may in the future revise our position as circumstances change or as we evaluate the actual impact of your disclosures on national security.

If we revise our position, we will notify you. We would retain the right to bring an appropriate enforcement action with respect to any future disclosures you make after you receive a notification of our change in position.

Thank you again for discussing your proposals with us in an effort to reach an agreement that promotes transparency without jeopardizing our national security responsibilities to the public.

Sincerely,



Andrew Weissmann
General Counsel

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

March 19, 2013

Bryan Schilling
Attorney
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Re: Microsoft's Pending Transparency Report

Dear Mr. Schilling:

Thank you for your proposal to publish certain limited information about the number of national security letters that Microsoft receives.

We do not intend to seek to enforce the non-disclosure provisions of the national security letter statute with respect to the proposed disclosures outlined in your letter dated March 14, 2013 (the "Letter"). This position is an exercise of FBI discretion in light of current circumstances and the precise contours of your Letter. Accordingly, our decision does not reflect the FBI's position with respect to potential disclosures by Microsoft that differ in any respect from the disclosures outlined in your Letter. Nor is our decision a precedent for disclosures by any other company that is in receipt of national security letters from the FBI, even if the disclosures were made in the manner that you have proposed in your Letter. The national security implications of disclosures related to the receipt of national security letters may vary depending on the identity of the company that is making the disclosure and the overall number of disclosures by different companies. For this reason, if other companies also seek to disclose information about the volume of national security letters that they receive, that may alter our calculus about the implications of disclosures by Microsoft. In addition, our current determination is based on our prediction about the potential national security consequences of the disclosures outlined in your letter. We may in the future revise our position as circumstances change or as we evaluate the actual impact of your disclosures on national security.

We understand from your Letter that you will coordinate with us before making any additional public disclosures about the volume of national security letters you receive, beyond disclosures for the years and in the manner outlined in your Letter.

Thank you again for coordinating your proposal with us. We appreciate your efforts to reach an agreement that promotes transparency without jeopardizing our national security responsibilities to the public.

Sincerely,

Andrew Weissmann
General Counsel

(U) ATTACHMENT "B"

U.S. Department of Justice

Federal Bureau of Investigation

Office of the General Counsel

Washington, D.C. 20535

June 14, 2013

Mr. John Frank
Vice President/Deputy General Counsel
Office of the General Counsel
Microsoft Corporation
1 Microsoft Way
Redmond, WA 98052

Re: Microsoft's Pending Transparency Report

Dear Mr. Frank:

We appreciate your discussions with us about your proposal to disclose certain information about the volume of legal process Microsoft receives.

As we discussed during our phone call on June 14, 2013, we do not intend to seek enforcement[1] of the non-disclosure provisions associated with any legal process, including FISA orders, so long as Microsoft agrees to aggregate data for all of the legal process it received in intervals of six months, beginning with the period ending December 31, 2012, from any and all government entities in the United States (including local, state, and federal, and including criminal and national security-related requests) into bands of 1000, starting at zero, and broken down into two categories: the number of requests and the number of user accounts for which data was requested.

This position is an exercise of FBI discretion in light of current circumstances and the precise contours of this letter. Accordingly, our decision does not reflect the FBI's position with respect to potential disclosures by Microsoft that differ in any respect from the disclosures outlined in this letter. Nor is our decision a precedent for disclosures by any other company that is in receipt of such process, even if the disclosures were made in the manner that is proposed in this letter. The national security implications of disclosures related to the receipt of such process may vary depending on the identity of the company that is making the disclosure and the overall number of disclosures by different companies. For this reason, if other companies also seek to disclose information about the volume of such process that they receive, that may alter our

[1] The FBI does not have the authority to negate a court order, nor can we bind state or local authorities.

calculus about the implications of disclosures by Microsoft. In addition, our current determination is based on our prediction about the potential national security consequences of the disclosures and as such we may in the future revise our position as circumstances change or as we evaluate the actual impact of your disclosures on national security.

This letter further commits Microsoft to coordinate with us before making any additional public disclosures about the volume of legal process you receive, beyond the contours outlined in this letter. If we revise our position, we will notify you. We would retain the right to bring an appropriate enforcement action with respect to any future disclosures you make after you receive a notification of our change in position.

Thank you again for coordinating your proposal with us. We appreciate your efforts to reach an agreement that promotes transparency without jeopardizing our national security responsibilities to the public.

Sincerely,

Andrew Weissmann
General Counsel

U.S. Department of Justice

Federal Bureau of Investigation

Office of the General Counsel

Washington, D.C. 20535

June 17, 2013

Mr. Aaron Altschuler
Vice President/Associate General Counsel
Yahoo, Inc.
701 First Avenue
Sunnyvale, CA 94089

Re: Yahoo Inc.'s Transparency Report

Dear Mr. Altschuler:

We appreciate your discussion with us about your proposal to disclose certain information about the volume of legal process Yahoo, Inc. (Yahoo) receives.

As we discussed during our phone call on June 17, 2013, we do not intend to seek enforcement[1] of the non-disclosure provisions associated with any legal process, including FISA orders, in connection with the aggregate data described below, so long as Yahoo aggregates data for all of the legal process it received for intervals of six months, with the first period covering December 1, 2012, through May 31, 2013, from any and all government entities in the United States (including local, state, and federal, and including criminal and national security-related requests) into bands of 1000, starting at zero, and which you may break down into one or both of the following two categories: the number of requests and the number of user accounts for which data was requested.

This position is an exercise of FBI discretion in light of current circumstances and the precise contours of this letter. Accordingly, our decision does not reflect the FBI's position with respect to potential disclosures by Yahoo that differ in any respect from the disclosures outlined in this letter. Nor is our decision a precedent for disclosures by any other company that is in receipt of such process, even if the disclosures were made in the manner that is proposed in this letter. The national security implications of disclosures related to the receipt of such process may vary depending on the identity of the company that is making the disclosure and the overall number of disclosures by different companies. For this reason, if other companies also seek to disclose information about the volume of such process that they receive, that may alter our

[1] The FBI does not have the authority to negate a court order, nor can we bind state or local authorities.

calculus about the implications of disclosures by Yahoo. In addition, our current determination is based on our prediction about the potential national security consequences of the disclosures and as such we may in the future revise our position as circumstances change or as we evaluate the actual impact of your disclosures on national security.

This letter further commits Yahoo to coordinate with us before making any additional public disclosures about the volume of legal process you receive, beyond the contours outlined in this letter. If we revise our position, we will notify you. We would retain the right to bring an appropriate enforcement action with respect to any future disclosures you make after you receive a notification of our change in position.

Thank you again for coordinating your proposal with us. We appreciate your efforts to reach an agreement that promotes transparency without jeopardizing our national security responsibilities to the public.

Sincerely,

Andrew Weissmann
General Counsel

U.S. Department of Justice

Federal Bureau of Investigation

Office of the General Counsel

Washington, D.C. 20535

June 14, 2013

Ted Ullyot
General Counsel
Facebook
1601 Willow Road
Menlo Park, CA 94025

Re: Facebook's Pending Transparency Report

Dear Mr. Ullyot:

We appreciate your discussions with us about your proposal to disclose certain information about the volume of legal process Facebook receives.

As we discussed during our phone call on June 14, 2013, we do not intend to seek enforcement[1] of the non-disclosure provisions associated with any legal process, including FISA orders, so long as Facebook agrees to aggregate data for all of the legal process it received for intervals of six months, beginning with the period ending December 31, 2012, from any and all government entities in the United States (including local, state, and federal, and including criminal and national security-related requests) into bands of 1000, starting at zero, and broken down into two categories: the number of requests and the number of user accounts for which data was requested.

This position is an exercise of FBI discretion in light of current circumstances and the precise contours of this letter. Accordingly, our decision does not reflect the FBI's position with respect to potential disclosures by Facebook that differ in any respect from the disclosures outlined in this letter. Nor is our decision a precedent for disclosures by any other company that is in receipt of such process, even if the disclosures were made in the manner that is proposed in this letter. The national security implications of disclosures related to the receipt of such process may vary depending on the identity of the company that is making the disclosure and the overall number of disclosures by different companies. For this reason, if other companies also seek to disclose information about the volume of such process that they receive, that may alter our calculus about the implications of disclosures by Facebook. In addition, our current determination is based on our prediction about the potential national security consequences of

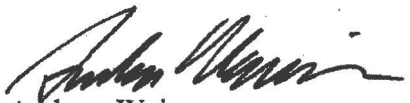
[1] The FBI does not have the authority to negate a court order, nor can we bind state or local authorities.

the disclosures and as such we may in the future revise our position as circumstances change or as we evaluate the actual impact of your disclosures on national security.

This letter further commits Facebook to coordinate with us before making any additional public disclosures about the volume of legal process you receive, beyond the contours outlined in this letter. If we revise our position, we will notify you. We would retain the right to bring an appropriate enforcement action with respect to any future disclosures you make after you receive a notification of our change in position.

Thank you again for coordinating your proposal with us. We appreciate your efforts to reach an agreement that promotes transparency without jeopardizing our national security responsibilities to the public.

Sincerely,



Andrew Weissmann
General Counsel

(U) ATTACHMENT "C"

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 13526, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 13526, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of sections 641, 793, 794, 798, *952 and 1924, title 18, United States Code; *the provisions of section 783(b), title 50, United States Code; and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of sections 793 and/or 1924, title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

(Continue on reverse.)

11. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 13526 (75 Fed. Reg. 707), or any successor thereto section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b) (8) of title 5, United States Code, as amended by the Whistleblower Protection Act of 1989 (governing disclosures of illegality, waste, fraud , abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); sections 7(c) and 8H of the Inspector General Act of 1978 (5 U.S.C. App.) (relating to disclosures to an inspector general; the inspectors general of the Intelligence Community. and Congress); section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 403-3h(g)(3) (relating to disclosures to the inspector general of the Intelligence Community); sections 17(d)(5) and 17(e)(3) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403g(d)(5) and 403q(e)(3)) (relating to disclosures to the Inspector General of the Central Intelligence Agency and Congress); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, *952 and 1924 of title 18, United States Code, and *section 4 (b) of the Subversive Activities Control Act of 1950 (50 U.S.C. section 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

12. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Part 2001 , section 2001 .80(d)(2)) so that I may read them at this time, if I so choose.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER *(See Notice below)*

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) *(Type or print)*

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		**THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.**	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS *(Type or print)*		NAME AND ADDRESS *(Type or print)*	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS *(Type or print)*	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Public Law 104-134 (April 26, 1996). Your SSN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above or to determine that your access to the information indicated has been terminated. Furnishing your Social Security Number, as well as other data, is voluntary, but failure to do so may delay or prevent you being granted access to classified information.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.2, 1.3, and 14(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classifjed information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, * the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER *(See Notice below)*

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) *(Type or Print)*

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS *(Type or print)*		NAME AND ADDRESS *(Type or print)*	

SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS *(Type or print)*	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.