

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

PROJECT FOR PRIVACY AND
SURVEILLANCE ACCOUNTABILITY, INC.,

Plaintiff,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

No. 1:22-cv-1812-RC

PLAINTIFF'S CROSS-MOTION FOR SUMMARY JUDGMENT

Pursuant to Federal Rule of Civil Procedure 56, Plaintiff Project for Privacy and Surveillance Accountability respectfully requests that the Court enter summary judgment in its favor in this Freedom of Information Act matter. As demonstrated in the accompanying memorandum, the Defendant agencies have not come close to satisfying their statutory obligations under FOIA. Rather, each agency flatly refused to conduct any search for responsive records, relying on an untenable expansion of the *Glomar* doctrine. As Congress clearly mandated that agencies must conduct a search for responsive records in response to a valid FOIA request, summary judgment should be entered for Plaintiff.

August 4, 2023

Respectfully submitted,

/s/ Gene C. Schaerr

GENE C. SCHAERR (D.C. Bar No. 416368)

Brian J. Field (D.C. Bar No. 985577)

SCHAERR | JAFFE LLP

1717 K Street NW, Suite 900

Washington, DC 20006

(202) 787-1060

gschaerr@schaerr-jaffe.com

Counsel for Plaintiff

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

PROJECT FOR PRIVACY AND
SURVEILLANCE ACCOUNTABILITY, INC.,

Plaintiff,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

No. 1:22-cv-1812-RC

**PLAINTIFF'S MEMORANDUM OF POINTS AND AUTHORITIES IN
SUPPORT OF ITS CROSS-MOTION FOR SUMMARY JUDGMENT AND
IN OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT**

TABLE OF CONTENTS

INTRODUCTION 1

BACKGROUND 2

LEGAL STANDARD..... 3

ARGUMENT 4

I. Even if *Glomar* Responses are Lawful Under FOIA, Defendants Cannot Rely on *Glomar* here..... 4

II. Defendants Fail to Demonstrate That Exemption 1 Permits Them to Avoid Conducting a Search Under the *Glomar* Doctrine. 8

 A. Defendants fail to establish that all the withheld information satisfies EO 13526’s substantive criteria. 9

 B. Defendants also fail to establish compliance with EO 13526’s several procedural criteria. 14

III. Defendants Likewise Fail to Demonstrate that Exemption 3 Permits Them to Avoid Conducting a Search under *Glomar*. 18

IV. Defendants Also Fail to Demonstrate that Exemptions 6, 7(C), and 7(E), Permit Them to Avoid Conducting a Search under the *Glomar* Doctrine. 20

 A. The DOJ and the FBI fail to meet their burden of making a threshold showing that all responsive records were compiled for law enforcement purposes. 21

 B. DOJ and the FBI also fail to meet their burden of showing that Exemptions 7(C) and 6 would cover all responsive records. 22

 C. The DOJ and the FBI fail to establish that a FOIA search would cause harm cognizable under an appropriately narrow construction of Exemption 7(E). 25

CONCLUSION..... 27

TABLE OF AUTHORITIES

Cases

ACLU v. CIA,
710 F.3d 422 (D.C. Cir. 2013)..... 5

ACLU v. U.S. Dep’t of Def.,
628 F.3d 612 (D.C. Cir. 2011)..... 6

Bartko v. U.S. Dep’t of Just.,
898 F.3d 51 (D.C. Cir. 2018)..... *passim*

Citizens for Resp. & Ethics in Wash. v. U.S. Dep’t of Just.,
746 F.3d 1082 (D.C. Cir. 2014)..... 24

Davin v. U.S. Dep’t of Just.,
60 F.3d 1043 (3d Cir. 1995) 25

Davis v. Dep’t of Just.,
460 F.3d 92 (D.C. Cir. 2006)..... 24

Dep’t of Just. v. Reps. Comm. for Freedom of Press,
489 U.S. 749 (1989)..... 23

Forest Serv. Emps. for Env’t Ethics v. U.S. Forestry Serv.,
524 F.3d 1021 (9th Cir. 2008) 24

Jud. Watch, Inc. v. U.S. Secret Serv.,
726 F.3d 208 (D.C. Cir. 2013)..... 4

Jud. Watch, Inc. v. U.S. Dep’t of Def.,
715 F.3d 937 (D.C. Cir. 2013)..... 8, 11, 15

Kissinger v. Reps. Comm. for Freedom of the Press,
445 U.S. 136 (1980)..... 17

Mobley v. CIA,
806 F.3d 568 (D.C. Cir. 2015)..... 3, 15, 16

People for the Ethical Treatment of Animals v. Nat’l Inst. of Health,
745 F.3d 535 (D.C. Cir. 2014)..... 5, 6, 14

Perry v. Block,
684 F.2d 121 (D.C. Cir. 1982)..... 3

Project for Privacy & Surveillance Accountability, Inc. v. U.S. Dep’t of Justice,
633 F. Supp. 3d 108 (D.D.C. 2022)..... 5, 10, 15

Ray v. Turner,
587 F.2d 1187 (D.C. Cir. 1978)..... 4

Ripskis v. HUD,
746 F.2d 1 (D.C. Cir. 1984)..... 22

Roth v. U.S. Dep’t of Just.,
642 F.3d 1161 (D.C. Cir. 2011)..... 5

<i>SafeCard Servs., Inc. v. SEC</i> , 926 F.2d 1197 (D.C. Cir. 1991).....	24
<i>Schaerr v. U.S. Dep’t of Just.</i> , 69 F.4th 924 (D.C. Cir. 2023).....	7
<i>Shapiro v. U.S. Dep’t of Just.</i> , 153 F. Supp. 3d 253 (D.D.C. 2016).....	5, 6
<i>Shapiro v. CIA</i> , 170 F. Supp. 3d 147 (D.D.C. 2016).....	19
<i>Vazquez v. U.S. Dep’t of Just.</i> , 887 F. Supp. 2d 114 (D.D.C. 2012).....	26
<i>Wolf v. CIA</i> , 473 F.3d 370 (D.C. Cir. 2007).....	3, 6
Statutes	
5 U.S.C. § 552.....	8, 15
18 U.S.C. § 798.....	18, 20
50 U.S.C. § 3605.....	19
National Security Act.....	18
National Security Agency Act of 1959.....	18, 19
Rule	
Fed. R. Civ. P. 56.....	3
Other Authorities	
Executive Order 13526	<i>passim</i>
Fourth Amendment is Not For Sale Act, S.1265 & H.R. 2738, 117th Cong. (2021).....	2
S. Select Comm. to Study Gov’tl Operations, <i>Intelligence Activities and the Rights of Americans</i> , S. Rep. No. 94-755, Book II (1976)	13

INTRODUCTION

Through this Freedom of Information Act case, the Project for Privacy and Surveillance Accountability, Inc. (“PPSA”) seeks to learn the extent to which the United States Intelligence Community’s (“IC”) openly acknowledged bulk purchasing and use of commercially available information (“CAI”) has swept in members of the Legislative Branch. As the Office of the Director of National Intelligence recently recognized, the IC’s longstanding practice of collecting consumer and other publicly available information without a warrant, when aided by third-party bulk data collection services, facilitates an alarming and unprecedented intrusion into the most intimate details of Americans’ lives. Absent judicial oversight through the Fourth Amendment, FOIA provides one of the few remaining mechanisms for the public to hold the IC accountable. But it only works if the agencies comply with their statutory obligations to search for and disclose responsive, non-exempt records.

Here, the various Defendant agencies failed to do so, refusing even to conduct a search. Rather, each Defendant relies on an aggressive and untenable application of the already-tenuous *Glomar* doctrine. And, again without conducting any search to confirm the accuracy of their assertions, each Defendant asserts that identifying the existence or non-existence of responsive records would result in harm. Of course, it is equally possible that there are records for which no harm would befall the agency by disclosing their existence. But Defendants have decided to hide behind the growing practice of blindly asserting *Glomar* to escape the requirements Congress placed on federal agencies through FOIA.

That practice is itself unlawful under FOIA. But it is particularly inappropriate here, considering the IC’s own extensive public admissions—both on the IC’s widespread use of commercially available information, and on the IC’s ignorance of its own CAI practices. Contrasted with those admissions, the Defendants’ boilerplate allegations here of inevitable harm

fail to satisfy their burden of justifying their refusal to search for and produce responsive, non-exempt records.

Thus, the Court should deny Defendants' motion for summary judgment and grant PPSA's cross-motion. Only after Defendants conduct the searches FOIA requires will the public be any closer to knowing about the IC's acquisition of CAI regarding past and current members of the Legislative Branch.

BACKGROUND

PPSA's FOIA request concerns records about government acquisition of CAI—information that, though treated as public for Fourth Amendment purposes, can now be aggregated and analyzed in bulk to facilitate potentially inescapable surveillance into the most private aspects of modern life.

By letters dated July 26, 2021, PPSA submitted FOIA requests to each of the Defendants regarding the IC's acquisition and use of CAI. Compl., Exs. A, E, H, P (ECF Nos. 1-1, 1-5, 1-8, 1-16). Those letters requested all documents “regarding the obtaining, by any element of the intelligence community from a third party in exchange for anything of value, of any covered customer or subscriber record or any illegitimately obtained information regarding” any past or current member of congressional judicial committees listed in each letter.¹ *Id.* at 2; Am. Compl. ¶¶ 12, 13, 18, 23, 32, 38. (ECF No. 23).

With refreshing candor, the ODNI recently acknowledged that “the IC does not currently have sufficient visibility into its own acquisition and use of CAI across its 18 elements,” and that

¹ The requests defined the terms “covered customer or subscriber record”; “illegitimately obtained information”; “intelligence community”; “obtain in exchange for anything of value”; and “third party” consistently with definitions used in the Fourth Amendment is Not For Sale Act, S.1265 & H.R. 2738, 117th Cong. (2021), proposed legislation that would place greater restrictions on IC purchases of commercially available information. *See, e.g.*, ECF Nos. 1-1, 1-5, 1-8, 1-16, at 1.

prior inquiries into those practices “did not return comprehensive and reliable results.” Pl.’s Stmt. of Facts ¶ 24 (“Pl.’s Stmt.”). With that substantial caveat, the ODNI acknowledged that the IC “currently acquires a significant amount” of CAI which, as a “resource available to the general public,” is also available to foreign governments and “adversaries.” *Id.* ¶ 20; *see also id.* at ¶ 15. The IC also admitted that: (i) “CAI may [] be used for purposes other than intelligence collection and analysis,” *id.* ¶ 22; (ii) current practices do not “substantially restrict the purchase and use of such information for mission purposes,” *id.* ¶ 6; and (iii) as in previous examples of known surveillance abuse, government officials could “abuse [] CAI held by the IC” to “facilitate blackmail, stalking, harassment, and public shaming,” *id.* ¶ 23.

But even with those admissions of CAI’s public availability and of the IC’s failed oversight of its own CAI uses and abuses, each Defendant refused even to search for responsive records. Rather, the Defendants—NSA, CIA, DOJ (including its component the FBI), and ODNI—issued so-called *Glomar* responses, relying on Exemption 1, and, in some instances, also invoking Exemptions 3, 6, 7(C), and 7(E). *See generally* Defs.’ Mot. for Summary J. at 6–7 (ECF No. 26) (“Defs.’ MSJ”).

LEGAL STANDARD

Summary judgment is appropriate when “there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). “To meet this exacting standard in a FOIA suit,” the D.C. Circuit requires that “the defending agency must prove that each document that falls within the class requested either has been produced, is unidentifiable, or is wholly exempt from the FOIA’s inspection requirements.” *Perry v. Block*, 684 F.2d 121, 126 (D.C. Cir. 1982) (cleaned up). And the agency bears the burden of justifying the application of any exemptions, “which are exclusive and must be narrowly construed.” *Mobley v. CIA*, 806 F.3d 568, 580 (D.C. Cir. 2015); *see also Wolf v. CIA*, 473 F.3d 370, 374 (D.C. Cir. 2007) (courts must

construe FOIA exemptions “narrowly,” in keeping with “FOIA’s broad disclosure policy”). If the agency’s affidavits or declarations in support of summary judgment fail to provide “reasonable specificity of detail rather than merely conclusory statements,” or if they are “called into question by contradictory evidence in the record or by evidence of agency bad faith,” summary judgment in favor of the agency is not appropriate. *Jud. Watch, Inc. v. U.S. Secret Serv.*, 726 F.3d 208, 215 (D.C. Cir. 2013) (quotation marks and citation omitted). Moreover, even without a “finding or even tentative finding of bad faith,” a court conducting *de novo* review of an agency’s exemption claims may take into account government officials’ “inherent tendency to resist disclosure.” *Ray v. Turner*, 587 F.2d 1187, 1195 (D.C. Cir. 1978) (*per curiam*).

ARGUMENT

Unlike more complicated FOIA cases, this case presents a very straightforward question: Does FOIA require agencies to search for records responsive to a valid FOIA request? The answer, made clear by FOIA’s text, is a resounding yes. And, because there is no dispute about the validity of Plaintiff’s requests or about Defendants’ refusal to conduct a search, that is the end of the inquiry, and the Court must deny the Defendants’ motion for summary judgment and order the Defendants to conduct searches for responsive records. But further, Defendants’ boilerplate declarations fail to justify their reliance on Exemptions 1, 3, 6, or 7, which provides the Court yet another, alternative reason to deny Defendants’ motion.

I. Even if *Glomar* Responses are Lawful Under FOIA, Defendants Cannot Rely on *Glomar* here.

As discussed in the following sections, Defendants fail to justify their reliance on *Glomar* and Exemptions 1, 3, 6, and 7 when refusing to conduct any searches for responsive records. But this case presents the broader question of whether Defendants have satisfied their burden when invoking *Glomar* at the outset. They haven’t.

In “limited circumstances,” this Circuit’s *Glomar* cases permit an agency to refuse to confirm or deny the existence of records. *ACLU v. CIA*, 710 F.3d 422, 426 (D.C. Cir. 2013); accord *Bartko v. U.S. Dep’t of Just.*, 898 F.3d 51, 63 (D.C. Cir. 2018) (affirming that the circumstances justifying a *Glomar* response are “rare”). This, in turn, allows the agency to escape FOIA’s plain statutory language requiring the agency to search for and release responsive records. Cf. *Shapiro v. U.S. Dep’t of Just.*, 153 F. Supp. 3d 253, 273 (D.D.C. 2016) (observing that *Glomar*, as a “judicial gloss on FOIA,” is not described in the statute or its legislative history). As the D.C. Circuit recognizes, “[b]ecause *Glomar* responses are an exception to the general rule that agencies must acknowledge the existence of information responsive to a FOIA request and provide specific, non-conclusory justifications for withholding that information, they are permitted *only* when confirming or denying the existence of records would itself cause harm cognizable under an FOIA exception.” *Roth v. U.S. Dep’t of Just.*, 642 F.3d 1161, 1178 (D.C. Cir. 2011) (cleaned up; emphasis added).

However, Defendants have not provided any explanation to overcome the obvious conclusion that conducting an *internal* search for records does not itself constitute a disclosure that protected records do or do not exist. Rather, both the D.C. Circuit and this Court have recognized an agency’s ability to issue a “narrowed *Glomar* response” *after* searching for and disclosing any unprotected records. *People for the Ethical Treatment of Animals v. Nat’l Inst. of Health*, 745 F.3d 535, 545 (D.C. Cir. 2014) (“*PETA*”); *Project for Privacy & Surveillance Accountability, Inc. v. U.S. Dep’t of Justice*, 633 F. Supp. 3d 108, 123 (D.D.C. 2022) (“*PPSA*”) (Contreras, J.) (agency may consider “propriety of *Glomar*” response “only *after* conducting a search and assessing the fruits of such search” (emphasis added)). The widespread use of *post-search Glomar* responses demonstrates that an agency can fulfill its FOIA search mandate without confirming or denying

the existence of any sensitive information that may ultimately be found to fall within the *Glomar* doctrine.

The suggestion that *Glomar* excuses agencies from the general requirements of FOIA is misguided. Indeed, the D.C. Circuit requires that, “[i]n determining whether the existence of agency records *vel non* fits a FOIA exemption, courts apply the general exemption review standards established in non-*Glomar* cases.” *Wolf*, 473 F.3d at 374. Under those standards, the agency’s exemption justifications “need [to] be both plausible and logical.” *ACLU v. U.S. Dep’t of Def.*, 628 F.3d 612, 624 (D.C. Cir. 2011) (quotations omitted). Whenever “there exists a category of responsive documents for which a *Glomar* response would be unwarranted,” an agency’s “assertion of a blanket *Glomar* response ... cannot be sustained.” *PETA*, 745 F.3d at 545. Thus, even under *Glomar*, agencies are not “permitted ... to withhold—or to decline to confirm or to deny the existence of—any record or information that is *not* itself protected by a FOIA exemption or exclusion.” *Shapiro*, 153 F. Supp. 3d at 274 (original emphasis).

Rather, application of the judge-made *Glomar* doctrine is permitted “*only* when confirming or denying the existence of records would itself cause harm cognizable under an FOIA exception.” *Roth*, 642 F.3d at 1178 (emphasis added). Requiring Defendants to perform FOIA *searches* within the secrecy of their own siloes does not, by itself, compel the automatic disclosure of any information whatsoever, and without disclosure there can be no harm. Rather, post-search *Glomar* responses neatly demonstrate that searching for potentially unprotected records is procedurally and qualitatively distinct from confirming that protected records do or do not exist.

Because all of Defendants’ alleged harms are premised on the *disclosure* of protected information, *see* Defs.’ MSJ at 10, and because the initial step of conducting an intra-agency search makes no such disclosure, their arguments are neither logical nor plausible justifications for

shirking their duty to perform an internal search. Put another way, whatever the merits of Defendants' arguments about harm from disclosure at a later date, we are not yet at that point.

At present, Defendants give this Court no reason why they should not be required to conduct a search *before* considering the propriety of a subsequent *Glomar* response. And the D.C. Circuit's recent *Schaerr* decision provides Defendants no reprieve because that decision concerned "unmasking" and "upstreaming"—non-public forms of Foreign Intelligence Surveillance Act ("FISA") surveillance that necessarily target particular individuals. *See Schaerr v. U.S. Dep't of Just.*, 69 F.4th 924, 926–27 (D.C. Cir. 2023) (upstreaming "collects a target's communications"; agency may request non-consensual unmasking of United States person's identity only when "necessary to understand foreign intelligence information"). Here, unlike in the *Schaerr* case, the IC's bulk collection of CAI is neither wholly non-public nor intrinsically targeted at particular individuals. Thus, Defendants have no basis to claim that the mere act of searching their own records would necessarily reveal sensitive information.

The well-established safety of conducting intra-agency searches, standing alone, should be dispositive of these summary judgment proceedings. However, even if a search could be logically conflated with harmful disclosure, neither the Defendants nor their affiants plausibly eliminate the possibility of properly disclosable records. The IC's own admissions show that its CAI practices are both complex and troublingly opaque to the IC itself. Given those admissions, the Defendants' claimed confidence as to what an as-yet hypothetical search would reveal strains credulity. Because Defendants fail to plausibly eliminate categories of non-exempt records, they must conduct FOIA-mandated searches.

II. Defendants Fail to Demonstrate That Exemption 1 Permits Them to Avoid Conducting a Search Under the *Glomar* Doctrine.

Additionally, Defendants have not satisfied their burden of showing that Exemption 1 permits their refusal to search for responsive records. *See* Defs.’ MSJ at 11–15. Rather, Exemption 1 affords no justification for the government’s *Glomar* responses because their purported classification of the existence *vel non* of responsive records is neither “specifically authorized under criteria established by [Executive Order 13526]” nor “in fact properly classified pursuant to such [] order.” 5 U.S.C. § 552(b)(1)(A)–(B). Nor is any supposed interest implicated by an intra-agency search.

Where, as here, an agency fails to satisfy either of the “substantive and procedural criteria” for classification under Executive Order 13526 (“EO 13526”), it cannot rely on that order to justify its invocation of Exemption 1. *Jud. Watch, Inc. v. U.S. Dep’t of Def.*, 715 F.3d 937, 941 (D.C. Cir. 2013); *see also id.* at 943 (reiterating that an agency may withhold information under Exemption 1 only if that information is “classified in accordance with the procedural criteria of the governing Executive Order as well as its substantive terms” (quoting *Lesar v. U.S. Dep’t of Just.*, 636 F.2d 472, 483 (D.C. Cir. 1980))).

To satisfy the *substantive* criteria for a valid *Glomar* response, the classified information must not only “pertain to at least one of eight subject-matter classification categories,” but must also “reasonably be expected to cause some [defined] degree of harm to national security ... that is identifiable or describable.” *Jud. Watch*, 715 F.3d at 941 (citing EO 13526 §§ 1.1, 1.2, and 1.4). And, to satisfy the *procedural* criteria for such a response, an individual with classification authority must not only make the threshold reasonable-damage determination, but must take all steps necessary to properly classify the information by complying with the myriad procedural mandates described throughout the order. *See, e.g.*, EO 13526 §§ 1.1(a)(1) (requirement to classify

the information); 1.5(a) (requiring, “[a]t the time of original classification,” that the original classification authority “establish a specific date or event for declassification based on the duration of the national security sensitivity of the information”); 1.6 (requiring the classified information to be marked “in a manner that is immediately apparent” with: a classification level, the identity of the classifying authority, the agency and office of origin, declassification instructions, and a “concise reason for classification”); 1.7(a) (forbidding classification for certain prohibited purposes); 1.7(d) (imposing additional requirements for classifying previously undisclosed information “after an agency has received a request for it under the Freedom of Information Act”).

Because Defendants fail to satisfy either the substantive or procedural criteria of EO 13526, they have not carried their burden of relying on *Glomar* and Exemption 1.

A. Defendants fail to establish that all the withheld information satisfies EO 13526’s substantive criteria.

Defendants’ blanket *Glomar* responses fail to meet EO 13526’s substantive criteria because simply conducting a search, coupled with the possibility of issuing a post-search *Glomar* response, cannot plausibly be equated with inevitable disclosure, and thus cannot cause identifiable damage. In fact, the safety of conducting an internal search of CAI records is obvious from the IC’s own practices: ODNI Director Avril Haines recently declassified a 2022 report in which the IC investigated its own CAI practices (the “ODNI Report”). *See* Pl.’s Stmt. ¶¶ 10, 20–29. The authors of that report reviewed “representative samples” of CAI records in the IC’s possession, *id.* ¶ 24, and Director Haines subsequently confirmed that the “outside panel” had “stud[ied] ... the government’s purchase of data including sensitive data on Americans” and agreed that the panel’s report,” once scrubbed of classified information, “absolutely should” be made available to the public, *id.* ¶ 9. In other words, the IC conducted an internal record search, publicly confirmed that it had done so, and released the redacted fruits of that search—all without confirming or denying

the existence of sensitive information. The IC's own actions thus demonstrate that searching is not disclosure, and that an intra-agency search cannot cause identifiable and describable harm to national security. Exemption 1 therefore does not release Defendants from performing such a search here.

But even if conducting an internal search were equivalent to disclosing the existence *vel non* of responsive records, that mere fact could not reasonably be expected to cause identifiable and describable damage to national security. Rather, PPSA's request is broad, asking for any records "regarding" the obtaining of congressional members' commercial information. A request for a document *regarding* a certain subject, like a request for a document *concerning* a subject, "refers to the subject of the document." *PPSA*, 633 F. Supp. 3d at 121 (cleaned up). Such a request implicates not just "operational documents," but also "policy documents" whose acknowledged existence cannot reasonably be expected to damage national security. *Id.* That, by itself, defeats Defendants' blanket *Glomar* response under Exemption 1.

Moreover, the public nature of CAI at the heart of PPSA's request belies Defendants' suggestion (at 12) that the bare acknowledgment of responsive records could reasonably be expected to damage national security. At the risk of stating the obvious, CAI is fundamentally different from other intelligence sources and methods, including FISA surveillance, because CAI, as a "generally available resource," is neither proprietary nor exclusive to the IC, and thus is already available to "our adversaries." Pl.'s Stmt. ¶ 15. Thus, Defendants' entire premise of harm is misguided.

Indeed, the sources of CAI and the methods of obtaining and analyzing it are already publicly available. CAI is derived largely from public records and other publicly available information. *See id.* ¶¶ 12–14. Moreover, even though the data brokers from which the IC

purchases CAI may derive some of their information from nonpublic sources, neither the brokers nor their services are themselves secret. The declassified ODNI Report readily divulges “a list of the main sellers of CAI”—including familiar services like LexisNexis, Thomson Reuters, Oracle, and Equifax—“and a brief description of the types of information they make available.” *Id.* ¶ 18. The report also acknowledges that “[u]nclassified IC ... contracts for CAI can be found” at Sam.Gov, a publicly searchable U.S. government website, *id.* ¶ 21, and recognizes, as an example, that the website shows that Defendant FBI contracted with broker ZeroFox for social media CAI, *id.* Thus, as the ODNI Report confirms, the IC is capable of acknowledging the existence of substantial and specific information about its CAI practices without harming national security.

This public information, when coupled with the admission that the IC lacks comprehensive or reliable insight into how it actually uses CAI, destroys any confidence in the Defendants’ blanket claim (at 12–13) that acknowledging the mere existence of responsive records will “necessarily reveal” information about sensitive intelligence activities. To the contrary, the interplay of those two factors highlights multiple categories of records whose mere acknowledgement could not reasonably threaten national security. Indeed, by its own admission, “[t]he IC currently acquires a large amount of CAI,” including bulk information. Pl.’s Stmt. ¶ 21. And ODNI further acknowledged that this collection is not “substantially restrict[ed] [to] the purchase or use of such information for mission purposes.” *Id.* ¶ 6. Because it is already known that the IC casts an exceedingly wide net by engaging in bulk collection of CAI, which exceeds mission-related information, not all records responsive to PPSA’s request would necessarily reveal a targeted interest in any particular individual or objective. Here again, that is fatal to Defendants’ attempt to identify a “harm to national security.” *Jud. Watch*, 715 F.3d at 941 (citing EO 13526 §§ 1.1, 1.2, and 1.4).

If that were not enough, the IC’s current and past CAI practices are too varied, and too unexamined by the IC itself, to support Defendants’ assumption that the acknowledgment of any responsive record would necessarily harm national security. The IC’s approach to CAI is fragmented rather than unified, and “current practices vary more, and more unsystematically, than is best.” Pl.’s Stmt. ¶ 25. Unsurprisingly, then, the ODNI Report—a “thorough,” “90-day” investigation into the IC’s CAI practices by a panel of senior intelligence officials—ultimately abandoned hope of basing their report on “anything approaching a complete survey of the use of CAI by the IC.” *Id.* ¶¶ 10–11, 24. In other words, the IC does not know enough about its CAI practices to assert that conducting a search would necessarily cause an identifiable harm. Noting that “prior retrospective data calls ha[d] not fully succeeded,” and “did not return comprehensive and reliable results,” the report cited such “difficulties in accessing historical information about the use of CAI” to conclude, troublingly, that “the IC does not currently have sufficient visibility into its own acquisition and use of CAI across its 18 elements.” *Id.* at ¶ 24; *see also id.* at ¶ 25 (“The IC cannot understand and improve how it deals with CAI unless and until it knows what it is doing with CAI.”). If the ODNI Report, after a searching, 90-day investigation, admits that the IC does not fully know how it is using CAI, then the Defendants’ boilerplate assertions—based on no search whatever—cannot plausibly rule out the possibility that safely disclosable records exist.

What we do know is that the IC’s uses of CAI are varied, potentially inconsistent, and not necessarily tethered to its mission. The ODNI Report stresses that “policy questions concerning CAI are not one-dimensional” in part because the IC is able to use CAI “for purposes other than intelligence collection and analysis.” *Id.* ¶ 22. Two non-intelligence purposes include “supporting compliance with legal or policy requirements” and “building and training artificial intelligence models.” *Id.* However, the IC’s own internal audits show that there are insufficient guarantees that

IC elements always use CAI for proper, “mission purposes.” *Id.* ¶ 6. The ODNI Report admits that “[m]ission creep can subject CAI collected for one purpose to other purposes.” *Id.* ¶ 22. Once again, such acknowledged information gaps undermine Defendants’ blanket assertion of harm to national security.

Moreover, the ODNI Report recognizes that the IC’s opaque and fragmented CAI practices are ripe for abuse. *See* Pl.’s Stmt. ¶ 23 (“CAI Can Be Misused”). Not only does the ODNI worry that “sensitive insights gained through CAI could facilitate blackmail, stalking, harassment, and public shaming” if used “[i]n the wrong hands,” but cites “[d]ocumented examples” of IC abuses to admit that those “wrong hands” demonstrably include some “government officials.” *Id.* Those admissions are especially troubling, because documented cases of what the Church Report called “Political Abuse of Intelligence Information”—that is, collecting and disseminating information “in order to serve the purely political interests of an intelligence agency or the administration”—unfortunately date “back to the very outset of the domestic intelligence program.” S. Select Comm. to Study Gov’tl Operations, *Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755, Book II, at 225, 227 (1976), available at https://www.intelligence.senate.gov/sites/default/files/94755_II.pdf; *see generally id.* at 225–52 (documenting political surveillance abuses across successive administrations).

Because the IC’s warrantless CAI practices lack both internal transparency and systematization, Defendants cannot plausibly eliminate the possibility that a FOIA-mandated audit would reveal other such abuses. And such records of CAI misuse, perhaps with proper redaction, would not necessarily reveal proper IC activities or priorities.

At the very least, a search for such records—even if such a search were equivalent to disclosure, which it is not—would not *necessarily* reveal information harmful to national security.

As those “categor[ies] of responsive documents” do not meet the substantive requirements of EO 13526, Exemption 1 cannot sustain the FBI’s “assertion of a blanket *Glomar* response.” *PETA*, 745 F.3d at 545.

B. Defendants also fail to establish compliance with EO 13526’s several procedural criteria.

Similarly, Defendants’ failure to establish that they properly classified the existence *vel non* of responsive records also defeats their invocation of Exemption 1 for purposes of summary judgment. Defendants have shown, at best, that information regarding the possible existence of records was classified under a *portion* of EO 13526’s procedures. *See* Kiyosaki Decl. ¶ 21 (ECF No. 26-1) (information “has been properly classified under the procedures provided in Section 1.1”); Blaine Decl. ¶ 16 n.2 (ECF No. 26-2) (“Section 1.1(a) sets forth the procedural standards for classification, which have been satisfied in this case.”); Seidel Decl. ¶¶ 27–29 (ECF No. 26-4) (determining information to be classified only by reference to Sections 1.1 and 1.4); Breyan Decl. ¶ 12 (ECF No. 26-5) (relying on FBI’s classification determination); Koch Decl. ¶¶ 17–19 (ECF No. 26-3) (determining information to be classified only by reference to Sections 1.1 and 1.4). However, none of the Defendants’ affidavits provides the detail necessary to conclude that any of the Defendants completed all procedural steps required to classify that information before issuing their *Glomar* responses. For example, none of the affidavits establishes that the withheld information: (i) was accompanied by declassification instructions, EO 13526 §§ 1.5 and 1.6(a)(4); (ii) complied with the special procedures applicable to classifying information after that information has been requested through FOIA, EO 13526 § 1.7(d); or (iii) complied with any of the other transparency procedures required under the order.

The Defendants thus fail to show that the withheld information—the potential but unsearched-for existence or nonexistence of responsive records—was properly classified under the

only order invoked as a basis for Exemption 1. Instead, Defendants gloss over EO 13526's procedural requirements to claim incorrectly (at 11) that information is properly classified merely when an original classification authority "has determined [the information] to be classified" already. But just as someone cannot *declassify* information merely by wishing it so, no information becomes "properly classified," 5 U.S.C. § 552(b)(1)(B), without complying with all "procedural criteria" under the relevant order, *Jud. Watch*, 715 F.3d at 941. Because Defendants fail to show in "reasonable specificity of detail" that their *Glomar* responses satisfy all of EO 13526's procedural criteria, that order provides no logical or plausible basis for its invocation of Exemption 1, and their conclusory statements fail to qualify for summary judgment.

To be sure, this Court rejected similar arguments in *PPSA*, 633 F. Supp. 3d 108. But *PPSA* respectfully urges this Court to reconsider that decision. In its prior decision, the Court acknowledged that an agency issuing a *Glomar* response must comply with "four threshold requirements for proper classification" under EO 13526 § 1.1, but held that it need not comply with the order's "other procedural requirements," for example, those found in §§ 1.5–1.7. *PPSA*, 633 F. Supp. 3d at 118–19.

However, that non-textual distinction is incompatible with the plain language and structure of EO 13526, which expressly creates a uniform system for classification and declassification. In its prior rejection of such arguments, this Court adopted the holding in *Mobley v. CIA*, which reasoned that requiring an agency to comply with all of EO 13526's procedural requirements in the *Glomar* context would "appear to require agencies to create a record in response to a FOIA request," and that "would be contrary to longstanding FOIA law." 924 F. Supp. 2d 24, 48–49 (D.D.C. 2013), *aff'd*, 806 F. 3d 568 (D.C. Cir. 2015). But the reasoning in *Mobley* should not guide here, as it misapprehends prior precedents, which pose no such conflict. And that reasoning also

proves too much: It would just as easily absolve an agency from *ever* complying with EO 13526's numerous procedural requirements which, even outside the *Glomar* context, sometimes mandate the creation of new writings. Because EO 13526 does not exempt *Glomar* responses from any procedural requirements, Defendants' failure to show that they properly classified their withheld *Glomar* information prevents them from relying on Exemption 1.

Rather, the plain language of EO 13526 imposes a "*uniform* system for classifying ... and declassifying national security information." EO 13526 (emphasis added). As a single, uniform system, the order's substantive requirements are inextricable from its procedural requirements and give no indication that they were meant to be parsed selectively. For example, subsection 1.7(b) mandates that "[b]asic scientific research information not clearly related to the national security shall not be classified" (substantive), while the very next subsection 1.7(c)(1) stipulates that certain reclassifications must be "personally approved in writing" by an agency head (procedural). Even more crucially, subsection 1.7(a) imposes limitations that appear to be both substantive and procedural, forbidding both classification actions and omissions for prohibited purposes, including to "conceal violations of law, inefficiency, or administrative error," or to "prevent embarrassment to a person, organization, or agency." *Id.* §1.7(a).

Notwithstanding *Mobley* and this Court's prior decision in *PPSA*, the Defendants recognize that the procedural requirements of Section 1.7 are applicable to their *Glomar* decisions. *See* Kiyosaki Decl. ¶¶ 23, 26; Blaine Decl. ¶ 22; Seidel Decl. ¶ 33; Koch Decl. ¶ 19. And yet, Defendants point to nothing under EO 13526's uniform system that allows them to selectively comply with some of the order's procedural requirements but not others.

Mobley's supposed conflict between the demands of the Order's plain text and the principle that "FOIA does not require an agency to create or retain documents" is illusory, based on a simple

misapprehension of the language articulating that principle. 924 F. Supp. 2d at 48 (internal quotation marks and citations omitted). Simply put, FOIA only mandates disclosure of documents already in the government’s possession; hence, responding agencies need not create new records *to disclose*. See *Kissinger v. Reps. Comm. for Freedom of the Press*, 445 U.S. 136, 152 (1980) (FOIA “only obligates [the government] to provide access to those [documents] which it in fact has created and retained”). But, in articulating that principle, the Supreme Court did not mean that FOIA absolves agencies from having to comply with procedural requirements created by *other* binding authorities, including EO 13526’s numerous requirements requiring written documentation of classification decisions. That would be an alarming interpretation, one that is antithetical to the transparency concerns animating FOIA in the first place.

Whether in the *Glomar* context or otherwise, full compliance with EO 13526 requires government agencies to fulfill numerous affirmative obligations to create classified documents.² Most pointedly, Section 3.6(b) of the Order specifically requires that some *Glomar* determinations be made “in writing.” *Id.* § 3.6(b). If *Mobley*’s anti-record-creation reasoning were correct in the *Glomar* context, it would not only contradict the *Glomar*-specific provisions of EO 13526 § 3.6(b), but it would also logically release agencies from following any of the order’s record-keeping provisions *under any circumstances*. Because that argument proves too much, this Court should reject *Mobley* and read FOIA to complement, rather than override, EO 13526’s procedural, record-keeping requirements.

² See, e.g., EO 13526 §§ 1.3(c)(4) (delegation of original classification authority must be “in writing”), 1.7(c)(1) (decisions to reclassify after declassification must be approved “in writing”); § 1.8(b) (mandating that agency leaders “shall establish procedures” for challenging classification decisions), 1.9(d) (agency heads must “provide a report summarizing the results of the classification guidance review” and release an unclassified version to the public), 2.2(a) (agencies “shall prepare classification guides”).

Finally, at the most practical level, there is no reason the Defendants could not have complied with all procedural criteria applicable to tangible records because every *Glomar* response leaves tangible records on which all necessary markings could be placed—including, at the very least, the original FOIA request, the agency’s *Glomar* letter to the requester, and the agency’s affidavit defending its *Glomar* decision. In short, there is no real or theoretical tension between FOIA and EO 13526’s procedural criteria. Thus, Defendants’ failure to plausibly show that their *Glomar* decisions were properly classified defeats their reliance on Exemption 1, and they must perform a FOIA search.

III. Defendants Likewise Fail to Demonstrate that Exemption 3 Permits Them to Avoid Conducting a Search under *Glomar*.

As to their Exemption 3 defense, the Defendants (except the DOJ’s National Security Division) invoke three statutes—the National Security Act, the National Security Agency Act of 1959, and the criminal provisions of 18 U.S.C. § 798—to justify their *Glomar*-based refusal to conduct a search for responsive records. Defs.’ MSJ at 15–18. But, while those statutes might justify the *withholding* or *redaction* of particular records, none of them shields the Defendants from their statutory duty to perform an initial FOIA search.

As to the National Security Act, Defendants suggest (at 16–17) that “the only question for a court is whether the agenc[ies have] shown that responding to a FOIA request can reasonably be expected to lead to unauthorized disclosure of intelligence sources and methods.” (quotation marks and citation omitted). Even if that were the right question, which it is not, the answer is no.

As PPSA already demonstrated, Defendants continue raising the wrong question. The question is not, as Defendants suggest, about the potential for “unauthorized disclosure of intelligence sources and methods.” The question is whether merely conducting a *search* “can reasonably be expected to lead to the unauthorized disclosure of intelligence sources and

methods.” But a search alone cannot disclose anything. With FOIA’s well-established Exemptions in place, and with the benefit of appropriate redaction, it is unreasonable to expect that the mere act of performing a FOIA search will, by itself, lead to the unauthorized disclosure of intelligence sources and methods. And, as demonstrated in Section II.A., CAI is already a publicly available resource, compiled by non-government companies from largely publicly available information, and accessible by the general public including U.S. adversaries. Further, the IC has already listed the major vendors of CAI, described their services, and acknowledged that unclassified CAI contracts, including with IC elements, are publicly searchable. Given the public nature of CAI, the Defendants cannot plausibly eliminate the possibility of responsive records the disclosure of whose existence (or not) would not threaten intelligence sources and methods, and so cannot avoid a search through a blanket *Glomar* response.

Likewise, the NSA’s reliance on the National Security Agency Act of 1959, while it might justify the withholding of particular records, also does not justify the agency’s wholesale refusal to search for records not covered by that statute. The Act protects from disclosure “information with respect to the [NSA’s] activities.” 50 U.S.C. § 3605(a). But PPSA’s request is far broader, seeking “all documents, reports, memoranda, or communications regarding” the obtaining of CAI regarding named individuals “by any element of the intelligence community,” regardless of whether those records relate to the NSA’s own activities. Am. Compl. ¶ 13. Thus, the NSA’s *Glomar* response is obviously inadequate with respect to records in the NSA’s possession that do not relate to NSA’s own activities. *See Shapiro v. CIA*, 170 F. Supp. 3d 147, 158–59 (D.D.C. 2016) (rejecting *Glomar* response to the extent NSA records did not reveal NSA’s own interest in named individual).

Finally, the NSA's reliance on 18 U.S.C. § 798 (at 18) is misguided because that statute protects only "classified information," meaning "information ... specifically designated ... for limited or restricted dissemination or distribution." 18 U.S.C. § 798(a), (b). But, as shown by the IC's own disclosures, not all government records related to CAI are classified. Further, as noted in Section II.B., neither the NSA nor any of the other Defendants has claimed, much less shown, that they complied with all the EO 13526 procedural criteria necessary to classify the fact of the existence or nonexistence of responsive records before issuing their *Glomar* responses. Thus, to the extent the NSA made a substantive determination that the fact of the existence of responsive records was properly classifiable without actually fulfilling all steps necessary to classify that fact, 18 U.S.C. § 798 provides no basis to invoke Exemption 3.

Because Defendants cite no statute that would justify their wholesale refusal to search for responsive records, Exemption 3 provides no basis for their blanket *Glomar* responses.

IV. Defendants Also Fail to Demonstrate that Exemptions 6, 7(C), and 7(E), Permit Them to Avoid Conducting a Search under the *Glomar* Doctrine.

The DOJ and FBI also err in relying upon Exemptions 6 and 7. As a categorical answer to a FOIA request, a *Glomar* response fails when it lacks a categorical justification. Here the Defendants cannot invoke either of Exemptions 7(C) or 7(E) to justify their *Glomar* responses because they fail to "make a threshold showing" that all of "the FOIA request seeks records compiled for law enforcement purposes." *Bartko*, 898 F.3d at 64 (quotation marks and citation omitted); *see also* 5 U.S.C. § 552(b)(7). But even if Defendants had made that showing, the Defendants also fail to justify their *Glomar* responses because they fail to "mak[e] an *across-the-board* showing" that any of Exemptions 6, 7(C), or 7(E) would justify the categorical withholding of all responsive records. *Bartko*, 898 F.3d at 64 (emphasis added).

A. The DOJ and the FBI fail to meet their burden of making a threshold showing that all responsive records were compiled for law enforcement purposes.

As to the first showing, the DOJ and FBI trip at the outset by failing to recognize their actual burden. Although they flatly claim (at 19) that “any records here at issue” would be “compiled for law enforcement purposes,” their conclusory statements avoid even acknowledging this Circuit’s two-part “law-enforcement-purpose inquiry,” much less explaining how their *Glomar* responses satisfy that established framework. *Bartko*, 898 F.3d at 64 (citation omitted). That inquiry “focuses on how and under what circumstances the requested files were compiled, and whether the files sought relate to anything that can fairly be characterized as an enforcement proceeding.” *Id.* (cleaned up). As the D.C. Circuit explains, “[t]o qualify as law enforcement records, the documents must arise out of investigations which focus directly on *specifically alleged* illegal acts which could, if proved, result in civil or criminal sanctions.” *Id.* (cleaned up; emphasis added). Thus, summary judgment is unavailable because the DOJ and FBI provide “no sufficient basis on which to make the threshold *Glomar* determination” that all withheld records meet this standard. *Id.* at 66.

Nor could they. First, PPSA’s request does not exclusively, or even primarily, seek records directly generated by any law enforcement investigation. Rather, it seeks *any* records “regarding” the obtaining of congressional CAI, including policy documents and records in the Defendants’ possession that were generated by third parties. And, because PPSA’s request encompasses records relating to *any* IC element, not merely the DOJ and FBI, the Defendants have no basis to assume, absent a search, that all responsive records in those agencies’ possession would relate to a law enforcement proceeding.

Moreover, as shown above, the IC’s own records openly acknowledge that the IC obtains CAI in bulk, and that not all CAI usage is targeted, serves intelligence functions, or is necessarily

mission-related. And, to the extent any government actors within the admittedly opaque and unsystematic IC umbrella abuse their warrantless CAI capabilities for illicit purposes, the responsive records generated by such practices would lack either “a rational nexus between the investigation and one of the agency’s law enforcement duties [or] a connection between an individual or incident and a violation of federal law.” *Bartko*, 898 F.3d at 64 (cleaned up).

In short, because not all responsive records in the DOJ and FBI’s possession are necessarily law enforcement records, the Defendants bear the burden of “showing on a case-by-case basis” that all requested records were actually compiled for law enforcement purposes. However, without even finding what records they have, the Defendants cannot begin to satisfy this burden, and their reliance on Exemption 7 fails from the start.

B. DOJ and the FBI also fail to meet their burden of showing that Exemptions 7(C) and 6 would cover all responsive records.

In addition to failing to satisfy Exemption 7’s threshold law-enforcement-purpose requirement, Defendants cannot invoke Exemption 7(C) or 6³ to justify their *Glomar* response because they fail to meet their secondary burden of “making an across-the-board showing that the privacy interest the government asserts categorically outweighs any public interest in disclosure.” *Bartko*, 898 F.3d at 64.

First, as PPSA has already demonstrated repeatedly, Defendants cannot plausibly explain how merely conducting an intra-agency *search* would cause any harm to any privacy interests protected by Exemption 7(C) or 6. That, by itself, defeats their blanket *Glomar* responses and compels a search.

³ The Defendants concede (at 18 n.2) that Exemption 6 provides even weaker support for their *Glomar* response. Exemption 6 “weights the scales in *favor* of disclosure,” thus undermining rather than supporting the Defendants’ categorical refusal. *Ripskis v. HUD*, 746 F.2d 1, 3 (D.C. Cir. 1984) (emphasis added).

Second, Defendants fail to recognize that the same diminished privacy interests that allegedly allow them to amass large quantities of bulk CAI without a warrant tip the scales against their withholding that same information. The IC purchases CAI without any meaningful Fourth Amendment oversight precisely because the government treats U.S. persons as having waived their privacy rights by surrendering their personal information to third parties. In other words, Defendants ignore any privacy interests when they want to *collect* massive amounts of data indiscriminately, but then turn around and try to revive such privacy interests to avoid *disclosing* their actions to the public. The Court should not countenance this blatant attempt to avoid accountability.

Further, even if Defendants had sufficiently demonstrated any privacy interests that a search would implicate, PPSA's request has always been focused on the government's potential abuse of its surveillance powers, and *not* on any potential wrongdoing of members of Congress themselves. *See, e.g.*, Compl., Ex. H at 1 (ECF No. 1-8) (PPSA "troubled by the extent to which U.S. law enforcement and intelligence agencies may be purchasing Americans' private data without meaningful court oversight"); *id.*, Ex. M at 5 (ECF No. 1-13) (invoking "potential agency misconduct" as grounds for disclosure); *id.* at 4 (noting "public's interest in knowing whether [law enforcement and intelligence] agencies surveilled the U.S. Congress"). That focus aligns with FOIA's well-recognized, central public interest—"the citizens' right to be informed about what their government is up to." *Dep't of Just. v. Repts. Comm. for Freedom of Press*, 489 U.S. 749, 773 (1989) (internal quotations omitted). That is why PPSA specifically and repeatedly indicated its willingness to receive "anonymized" and "redacted" production to avoid "disclos[ing] any agency interest (or lack thereof) in any particular individual." Compl., Ex. H at 7. Thus, the requests' purpose has always been recognizably focused on federal agencies' own conduct and potential

misconduct. Media reporting of both government CAI practices, *see, e.g., id.* at 1 n.1, and similar potential IC misconduct toward members of Congress, *see, e.g., Compl., Ex. M* at 6 n.5, demonstrate the clear public interest in this subject.

Against that well-recognized public interest, the closest the Defendants come to identifying a categorical privacy interest justifying their *Glomar* responses is to cite *SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197 (D.C. Cir. 1991). But *SafeCard*, at best, would only “authorize the redaction of the names and identifying information of private citizens,” *not* allow the Defendants to “withhold every responsive document *in toto*.” *Citizens for Resp. & Ethics in Wash. v. U.S. Dep’t of Just.*, 746 F.3d 1082, 1094 (D.C. Cir. 2014). Because that justification is by no means coextensive with PPSA’s request, it cannot support the Defendants’ *Glomar* responses.

Further, the varying balances between particular privacy interests and the public interest in disclosure defeats any across-the-board *Glomar* response. *See Bartko*, 898 F.3d at 67 (*Glomar* response failed where agency could not “establish that there would be a single answer to every balancing of interests involving any [responsive] records”). Here, not only do all the individuals falling within the scope of PPSA’s request have diminished privacy interests as public officeholders, *Forest Serv. Emps. for Env’t Ethics v. U.S. Forestry Serv.*, 524 F.3d 1021, 1025–26 (9th Cir. 2008) (already reduced privacy interest of public officials even more diminished for higher level officials), but their privacy interests vary based on a number of other personal factors—not least, whether they are still alive, *see Davis v. Dep’t of Just.*, 460 F.3d 92, 97–98 (D.C. Cir. 2006) (affirming that fact of death may diminish privacy interest in nondisclosure). The Defendants recognize as much, and thus defeat their own blanket *Glomar* responses, by expressly disclaiming any reliance on Exemptions 6 or 7(C) “for deceased individuals.” Defs.’ MSJ at 21 n.3; *see also* Seidel Decl. ¶ 47 (ECF No. 26-4) (recognizing that at least five of the individuals

named in PPSA's requests are deceased). But even for living individuals, the Defendants fail to acknowledge how privacy interests degrade over time, further undermining their categorical approach to a request for documents stretching back more than 15 years. *Davin v. U.S. Dep't of Just.*, 60 F.3d 1043, 1058 (3d Cir. 1995) (noting that some individuals' "privacy interest may become diluted by the passage of time").

Thus, the compelling public interest in knowing whether U.S. intelligence agencies purchase the sensitive personal data of their own Congressional overseers greatly outweighs any diminished privacy interests of those already prominent public figures. Against that strong interest in disclosure, the FBI fails to show that the varying factors diminishing the countervailing privacy interests would justify categorical withholding of all information in all responsive records. Their "vaporous justification" cannot justify their blanket denial. *Bartko*, 898 F.3d at 66.

C. The DOJ and the FBI fail to establish that a FOIA search would cause harm cognizable under an appropriately narrow construction of Exemption 7(E).

DOJ's reliance (at 22–23) on Exemption 7(E) also fails, largely because DOJ ignores that CAI purchases are both publicly known and publicly available. By trying to nonetheless characterize the acquisition of CAI as a protected law-enforcement technique, DOJ stretches Exemption 7(E) beyond the breaking point.

As an initial matter, and as explained above, Defendants give no explanation for why conducting an intra-agency search for unprotected records would cause any harm contemplated by Exemption 7(E). Once again, the indisputable safety of conducting an internal search, combined with the possibility of issuing a post-search *Glomar* response, defeats their preemptive blanket *Glomar* responses.

But even reaching the substance of their Exemption 7(E) arguments, that exemption cannot justify a blanket *Glomar* response because PPSA's request encompasses any responsive records

in the DOJ and FBI's possession concerning data purchasing by *any* IC element, not just law enforcement agencies like the FBI. Absent a search, neither the DOJ nor the FBI can eliminate the likelihood that they possess responsive records that reveal nothing about law enforcement techniques and procedures. Further, even with respect to records generated by the DOJ or FBI, their reliance on Exemption 7(E) is untenable.

Moreover, as explained above, both the existence of data brokers' CAI services and the IC's extensive use of those services are already generally "known to the public." Seidel Decl. ¶ 52. Even more specifically, FBI Director Christopher Wray admitted that the FBI has purchased "commercial database information," Pl.'s Stmt. ¶ 9, and unclassified FBI contracts for CAI are publicly accessible, *id.* ¶¶ 7–8, 21. The IC's extensive and detailed disclosures regarding the CAI marketplace and the IC's various uses of CAI demonstrate that at least piecemeal disclosure of these techniques and processes is possible, defeating a blanket *Glomar* response.

Furthermore, the FBI's concerns (at 22) about confirming the collection of information related to specific individuals cannot protect all responsive records given the IC's confirmations that agencies do not always purchase and analyze CAI in targeted ways, nor always use it for intelligence or even mission-related purposes. The Defendants' blanket rationales do not adequately address the piecemeal reality of the IC's CAI usage and cannot justify a searchless *Glomar* response. Because PPSA's request encompasses records compiled *other* than for law enforcement purposes, and because redaction is possible even for law enforcement records, merely performing a statutorily mandated search will not "reduce or nullify the[] effectiveness" of this already well-known technique. *Vazquez v. U.S. Dep't of Just.*, 887 F. Supp. 2d 114, 116 (D.D.C. 2012) (quotation marks and citations omitted), *aff'd*, No. 13-5197, 2013 WL 6818207 (D.C. Cir. 2013) (per curiam).

Finally, as mentioned above, the scope of PPSA's request clearly encompasses both operational and policy documents, and Defendants make no attempt to explain how, as a categorical matter, a search for the latter will reveal any law enforcement techniques or procedures. Absent a categorical showing, the FBI's blanket *Glomar* response cannot stand.

CONCLUSION

Judging from the IC's own admissions, it is likely that Defendants possess responsive records whose disclosure, perhaps after appropriate segregation and redaction, will pose no conceivable risks of the types of harms cognizable under FOIA's narrowly construed exemptions. Given the IC's own disclosure of records that are neither sensitive nor related to law enforcement purposes, Defendants cannot justify their blanket refusal even to search for records. And, because Defendants fail to meet their burden of justifying their refusal to search for records, they should be ordered to comply with their FOIA obligation to conduct thorough searches for records responsive to PPSA's request.

August 4, 2023

Respectfully submitted,

/s/ Gene C. Schaerr

GENE C. SCHAERR (D.C. Bar No. 416368)

Brian J. Field (D.C. Bar No. 985577)

SCHAERR | JAFFE LLP

1717 K Street NW, Suite 900

Washington, DC 20006

(202) 787-1060

gschaerr@schaerr-jaffe.com

Counsel for Plaintiff

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

PROJECT FOR PRIVACY AND
SURVEILLANCE ACCOUNTABILITY, INC.,

Plaintiff,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

No. 1:22-cv-1812-RC

**PLAINTIFF’S RESPONSE TO DEFENDANTS’ STATEMENT OF FACTS AND
PLAINTIFF’S COUNTER-STATEMENT OF MATERIAL FACTS NOT IN DISPUTE**

Pursuant to Local Civil Rule 7(h), Plaintiff the Project for Privacy and Surveillance Accountability, Inc. (“PPSA”) hereby responds to Defendants’ Statement of Material Facts Not in Dispute (ECF No. 26-7).

1. Not disputed
2. Not disputed
3. Not disputed
4. Not disputed
5. Not disputed

6. Plaintiff objects that (i) Plaintiff’s December 2022 request to the Justice Department’s National Security Division sought records created, altered, sent, or received “between January 1, 2008, and the date NSD conducts a search for responsive records” (Ex. S); and (ii) contrary to Defendants’ citations, the date ranges for Plaintiff’s requests can be found at the following citations: Complaint ¶¶ 13, 18, 23, 38; *id.*, Exs. A, E, H, P, S. The remainder of this paragraph is not disputed.

7. Not disputed

8. Not disputed

9. Plaintiff objects that the question of whether the Kiyosaki Declaration explains the basis for the NSD's *Glomar* response in a way sufficient to meet the NSD's burden under FOIA is a legal conclusion, not a statement of fact.

10. Not disputed.

11. Not disputed

12. Plaintiff objects that the question of whether the Blaine Declaration explains the basis for the CIA's *Glomar* response in a way sufficient to meet the CIA's burden under FOIA is a legal conclusion, not a statement of fact.

13. Not disputed

14. Not disputed

15. Plaintiff objects that the question of whether the Seidel Declaration explains the basis for the FBI's *Glomar* response in a way sufficient to meet the FBI's burden under FOIA is a legal conclusion, not a statement of fact.

16. Not disputed

17. Not disputed

18. Plaintiff objects that the question of whether the Tiernan Declaration explains the basis for the NSD's *Glomar* response in a way sufficient to meet the NSD's burden under FOIA is a legal conclusion, not a statement of fact.

19. This paragraph is grammatically ambiguous. To the extent that the paragraph may be construed to mean that the Office of Information Policy, via a letter dated September 22, 2022, provided a *Glomar* response to Plaintiff's request, that is not disputed.

20. Not disputed

21. Plaintiff objects that the question of whether the Breyan Declaration explains the basis for the OPI's *Glomar* response in a way sufficient to meet the OPI's burden under FOIA is a legal conclusion, not a statement of fact.

22. Plaintiff objects that, contrary to Defendants' citation to the Complaint, the details of ODNI's *Glomar* response can be found at Complaint ¶ 39. The remainder of this paragraph is not disputed.

23. Plaintiff objects that, contrary to Defendants' citation to the Koch Declaration, the details of Plaintiff's administrative appeal and the ODNI's response can be found at ¶ 11 of that declaration. The remainder of this paragraph is not disputed.

24. Plaintiff objects that the question of whether the Koch declaration explains the basis for the ODNI's *Glomar* response in a way sufficient to meet the ODNI's burden under FOIA is a legal conclusion, not a statement of fact.

Pursuant to Local Rule 7(h), PPSA respectfully submits the following Statement of Material Facts Not In Dispute.

1. By internal ODNI email dated March 1, 2021 ("Huebner Email"), Benjamin Huebner, Chief of the ODNI Office of Civil Liberties, Privacy, and Transparency, circulated a "white paper regarding commercially acquired information" that analyzed "how these procedures are being implemented across the IC" [U.S. Intelligence Community]. The Huebner Email is contained in Plaintiff's Exhibit 1. ODNI Off. of Civ. Liberties, Privacy, & Transparency, *Key Concepts Relevant to a Framework for the Intelligence Community's Acquisition and Use of*

Commercially Acquired Information (Mar. 2021) (the “ODNI White Paper”)¹ is contained in Plaintiff’s Exhibit 2.

2. The ODNI White Paper noted that, although “certain information may be commercially available,” an IC element “may use HUMINT or SIGINT means to collect the data in order to obfuscate the U.S. government’s acquisition of the data.” (Ex. 2 at 3). Thus, the paper used the term “commercially *acquired* information (CAI)” to refer to “those instances where an IC element has in fact acquired commercially available information through commercial means, whether or not that data is publicly available.” Ex. 2 at 3.

3. The ODNI White Paper also noted that “[n]ot all commercially available information constitutes publicly available information” because “[da]ta or other information sold exclusively to government entities constitutes commercially-available information, but not publicly available information.” (Ex. 2 at 3). The paper stated that “[t]his is a distinction with a significant difference [because] non-publicly available, commercially available information is subject to more restrictive acquisition, retention, and dissemination controls associated with other forms of collection, such as information acquired from tasked human sources.” Ex. 2 at 3.

4. The ODNI White Paper listed several categories of commercially acquired information including: (I) “Location Information”; (II) “Communications Content and Other Related Metadata” like “(a) Internet search terms used by individuals; (b) web-browsing data; and (c) bulk social media content that is publicly available”; (III) “Biometric Data,” including “bulk

¹ The ODNI disclosed the Huebner Email and ODNI White Paper to PPSA in response to a separate FOIA request, which is the subject of a separate lawsuit before this court: *Project for Privacy and Surveillance Accountability, Inc. v. The Office of the Director of National Intelligence*, 1:22-cv-2134-CRC (D.D.C.).

biometric data”; and (IV) “Other Bulk Data that May Allow for Inferences Regarding Constitutionally-Protected Activities.” Ex. 2 at 4–5.

5. The ODNI White Paper recommended developing a “CAI framework” that “should consider whether to prohibit or substantially restrict, as a matter of policy, the bulk collection of persistent mobile location information of individuals located in the United States.” The paper further stated:

Bulk purchase and use of such information currently presents the most significant privacy and civil liberties concerns. The capability to monitor, historically and persistently, the American populace at scale was likely unimaginable to the Founders. [...] The prevalence of cell phones, combined with the commonality of location-tracking mobile applications, severely limits the ability of individuals to opt out of such ubiquitous surveillance.

Ex. 2 at 7–8.

6. The ODNI White Paper concluded by recommending that “[t]he IC should also evaluate its purchase and use of bulk location information within the United States and determine whether to prohibit or substantially restrict the purchase and use of such information for mission purposes.” Ex. 2 at 9. Elsewhere, the paper noted that “while additional protections are required for VPS [volume, proportion, or sensitivity] data, there is no IC-wide guidance and limited IC element guidance regarding the types of collections that would meet the volume, proportion, or sensitivity standards that trigger these heightened requirements.” (Ex. 2 at 7). Thus, “the application of the heightened approval and handling requirements associated with VPS data”—even if such data is “commercially acquired or drawn from publicly available information”—“would help ensure such collection is restricted to that which is necessary to support the IC’s mission and that the resulting data is appropriately handled constituent with respect for privacy and civil liberties concerns.” Ex. 2 at 7.

7. In an online article dated March 27, 2023, Vice Media reported that in response to a FOIA request the FBI had disclosed a 2017 contract, Exhibit 3, between the FBI and Team Cymru, an information reseller, to obtain mass internet data (the “Cymru Contract”). *See* Joseph Cox, *Here is the FBI’s Contract to Buy Mass Internet Data*, Vice (Mar. 27, 2023, 9:00 AM), <https://tinyurl.com/3tyrudja> (providing link to contract). The contract, which Vice Media attached to its article, is contained in Plaintiff’s Exhibit 3.

8. The Cymru Contract, issued by the FBI Information Technology Contracts Unit, indicates that the FBI Cyber Division requisitioned “Commercially provided net flow information/data” for a two-month period, “09/15/2017 – 11/15/2017”, in exchange for \$76,450. Ex. 3 at 1, 2.

9. On March 8, 2023, in a public hearing before the U.S. Senate Select Intelligence Committee, the following exchange occurred between Senator Ron Wyden and FBI Director Christopher Wray:

WYDEN: Director Wray, does the FBI purchase U.S. phone geolocation information?

WRAY: So, to my knowledge, we, uh, do not currently purchase commercial database information that includes location data derived from internet advertising. I understand that we previously, as in the past, uh, purchased some such information for a specific national security pilot project, but that’s not been active for some time.

Testimony of FBI Dir. Christopher Wray before S. Select Intel. Comm., C-SPAN, at 00:10–00:40 (Mar. 8, 2023), <https://tinyurl.com/3c598cha>. In the same hearing, the following exchange occurred between Senator Wyden and Director of National Intelligence Avril Haines:

WYDEN: Director Haines, you convened an outside panel to study and make recommendations related to the government’s purchase of data including sensitive data on Americans. There has been a lengthy report that has been done here. Will you agree to release this report to the public?

HAINES: Thank you, Senator. I'll absolutely, uh, we'll have our folks review it for that purpose.

WYDEN: Is there any reason why it shouldn't be made available to the public?

HAINES: No, I think it absolutely should, as long as there's not classified information in it we'll provide it.

Testimony of Dir. of Nat'l Intel. Avril Haines before S. Select Intel. Comm., C-SPAN, at 01:08–01:41 (Mar. 8, 2023), <https://tinyurl.com/3c598cha>.

10. On June 14, 2023, Director of National Intelligence Avril Haines released an online statement titled “DNI Haines Statement on Declassified Report on Commercially Available Information” which stated, in part:

Given the increasing volume of data that is commercially available, I established a Senior Advisory Group Panel on Commercially Available Information and asked them to make recommendations to the Intelligence Community (IC) regarding how and under what circumstances the IC should use commercially available information, and in particular, to reflect on the existing framework for ensuring the protection of privacy and civil liberties. The panel prepared a thorough report, along with key recommendations, which we are now considering and working to implement.

Press Release, ODNI No. 15-23, Avril D. Haines, Dir. of Nat'l Intel., DNI Haines Statement on Declassified Report on Commercially Available Information (June 14, 2023), <https://tinyurl.com/2p9bh7de>. The bottom of the online statement contained a link to download the Declassified Report on Commercially Available Information. Off. of the Dir. of Nat'l Intel., Sr. Advisory Grp., Panel on Commercially Available Info., *Report to the Director of National Intelligence* (Jan. 27, 2022), <https://tinyurl.com/ukc4sd5z> (“ODNI Report”) (Exhibit 4).

11. The ODNI Report, described as a “90-day report on commercially available information (CAI),” was prepared by an ODNI “Senior Advisory Group Panel” and transmitted to

DNI Haines on January 27, 2022. Ex. 4 at 1, 3.² The report “addresses CAI that is available for purchase by the general public and as such is treated as a subset of publicly available information (PAI).” Ex. 4 at 3.

12. The ODNI Report quotes a 2013 GAO report to explain that sellers of CAI, also called “data brokers” or “information resellers,”

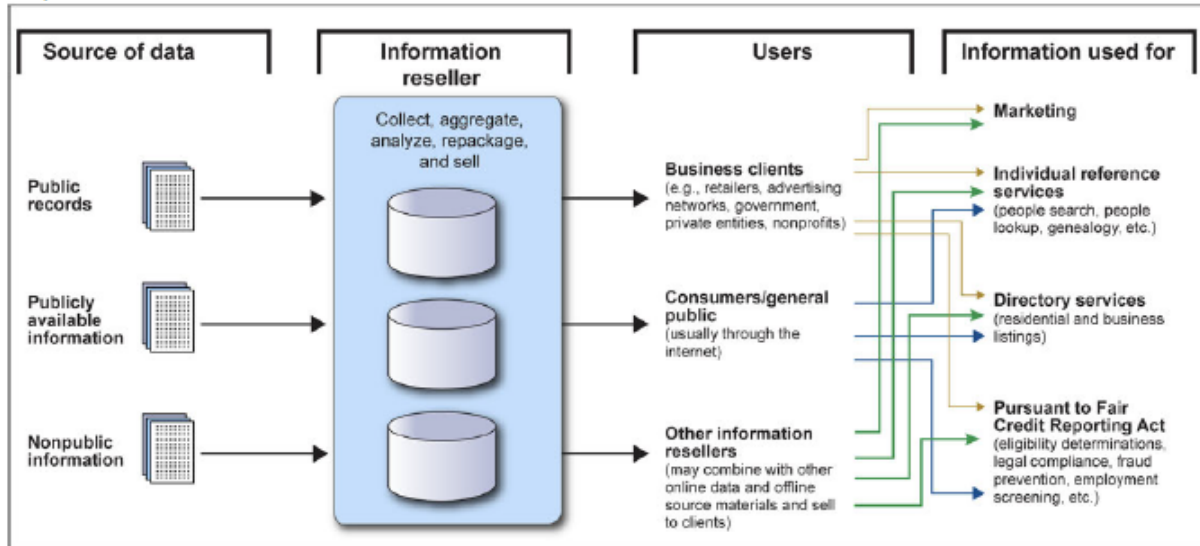
maintain large, sophisticated databases with consumer information that can include credit histories, insurance claims, criminal records, employment histories, incomes, ethnicities, purchase histories, and interests. Resellers largely obtain their information from public records, publicly available information (such as directories and newspapers), and nonpublic information (such as from retail loyalty cards, warranty registrations, contests, and web browsing).

Ex. 4 at 12–13 (quoting U.S. Gov’t Accountability Off., *GAO-14-251T, Information Resellers: Consumer Privacy Framework needs to Reflect Changes in Technology and the Marketplace 2* (Dec. 2013)).

13. The ODNI Report features a graphic that a GAO official used in June 2019 “to illustrate the development of and market for CAI” to the Senate Banking Committee, which is reprinted below:

² Although the ODNI Report was released as a single PDF, the document is comprised of several sub-documents, including a letter to DNI Haines, an Executive Summary, and the body of the report, which are all paginated separately. As such, page citations refer to the pagination inserted by counsel in the lower right corner.

Graph is Unclassified



Source: GAO. | GAO-19-621T

Ex. 4 at 13 (quoting U.S. Gov't Accountability Off., *GAO-19-621T, Consumer Privacy: Changes to Legal Framework Needed to Address Gaps* 3 (June, 2019) (statement of Alicia Puente Cackley, Dir. Fin. Mkts. & Cmty. Invs. before S. Comm. on Banking, Hous. & Urb. Affs.)).

14. The ODNI Report also quotes a 2014 FTC report to state:

Data brokers collect data from commercial, government, and other publicly available sources. Data collected could include bankruptcy information, voting registration, consumer purchase data, web browsing activities, warranty registrations, and other details of consumers' everyday interactions. Data brokers do not obtain this data directly from consumers, and consumers are thus largely unaware that data brokers are collecting and using this information. While each data broker source may provide only a few data elements about a consumer's activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer's life.

Ex. 4 at 13 (quoting Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and Accountability* iv (May 2014)).

15. The ODNI Report states that: "[t]here is today a large and growing amount of CAI that is available to the general public, including foreign governments (and their intelligence services) and private-sector entities, as well as the IC." Ex. 4 at 3. Elsewhere, the report states:

“There is also a growing recognition that CAI, as a generally available resource, offers intelligence benefits to our adversaries, some of which may create counter-intelligence risk for the IC.” Ex. 4 at 21.

16. The ODNI Report also cites a 2021 Duke University report analyzing 10 major data brokers that sell data on U.S. individuals. (Ex. 4 at 21 citing Jake Sherman, Duke Univ. Sanford Cyber Pol’y Program, *Data Brokers and Sensitive Data on U.S. Individuals: Threats to American Civil Rights, National Security, and Democracy* (2021) (“Duke Report”) (Exhibit 5)). The Duke Report is contained in Plaintiff’s Exhibit 5. The ODNI Report quotes the Duke Report to state: “Foreign intelligence organizations could acquire this data through a variety of means—including through front companies that could legally purchase the data from U.S. brokers ...—to build profiles on politicians, media figures, diplomats, civil servants, and even suspected or secretly identified intelligence operatives.” Ex. 4 at 21 (quoting Ex. 5 at 11).

17. The 10 major data brokers listed in the Duke Report are: Acxiom, LexisNexis, Nielsen, Experian, Equifax, CoreLogic, Verisk, Oracle, Epsilon, and the general category of “People-search” or “white pages” websites. Ex. 5 at 3; *see also id.* at 3–8. The ODNI Report also states: “As of this writing, major data brokers include Accenture, Acxiom [sic], CoreLogic, Epsilon, Intelius, LexisNexis, Oracle (Datalogix), Thomson Reuters, and Verisk.” Ex. 4 at 14.

18. The ODNI Report lists “a few examples of CAI offerings [that] illustrate the current nature of available offerings:

- (U) “Thomson Reuters CLEAR® is powered by billions of data points and leverages cutting-edge public records technology to bring all key content together in a customizable dashboard.”
- (U) LexisNexis offers more than “84B records from 10,000+ sources, including alternative data that helps surface more of the 63M unbanked/underbanked U.S. adults.”
- (U) Exactis has “over 3.5 billion records (updated monthly)” in its “universal data warehouse.”

- (U) PeekYou “collects and combines scattered content from social sites, news sources, homepages, and blog platforms to present comprehensive online identities.”

(Ex. 4 at 14). The conclusion to the report states that the report contains “a list of the main sellers of CAI and a brief description of the types of information they make available.” Ex. 4 at 46.

19. The ODNI Report states that market for CAI “includes significant information on U.S. persons, much of which can be acquired in bulk.” Ex. 4 at 14. It states that

[t]oday’s CAI is more revealing, available on more people (in bulk), less possible to avoid, and less well understood than traditional PAI [publicly available information]. ... Today, in a way that far fewer Americans seem to understand, and even fewer of them can avoid, CAI includes information on nearly everyone that is of a type and level of sensitivity that historically could have been obtained, if at all, only through targeted (and predicated) collection.

Ex. 4 at 24. The report also states that “[a]lthough CAI may be ‘anonymized,’ it is often possible (using other CAI) to deanonymize and identify individuals, including U.S. persons.” Ex. 4 at 11.

20. The ODNI Report states:

CAI clearly provides intelligence value, whether considered in isolation and/or in combination with other information, and whether reviewed by humans and/or by machines. The IC currently acquires a significant amount of CAI for mission-related purposes, including in some cases social medial data [redacted] and many other types of information. As a resource available to the general public, including adversaries, CAI also raises counter-intelligence risks for the IC. It also has increasingly important risks and implications for U.S. person privacy and civil liberties, as CAI can reveal sensitive and intimate information about individuals. Without proper controls, CAI can be misused to cause substantial harm, embarrassment, and inconvenience to U.S. persons.

Ex. 4 at 17.

21. The ODNI Report states: “The IC currently acquires a large amount of CAI. Unclassified IC and other contracts for CAI can be found at Sam.Gov, a U.S. government website that allows searching by agency or sub-agency and by keywords, among other things.” The report

notes, “[b]y way of example only,” that the website shows that the FBI contracted with ZeroFox for CAI related to “social media alerting.” Ex. 4 at 17.

22. The ODNI Report states: “It is important to recognize that in some cases, CAI may also be used for purposes other than intelligence collection and analysis.” (Ex. 4 at 17). As examples, the report says that “CAI may be useful in supporting compliance with legal or policy requirements,” and “in building and training artificial intelligence models.” Ex. 4 at 20. The report authors use these examples of non-analytic uses to demonstrate that “policy questions concerning CAI are not one-dimensional.” The report also states that “[m]ission creep can subject CAI collected for one purpose to other purposes that might raise risks beyond those originally calculated.” Ex. 4 at 21.

23. The ODNI Report recognizes that “CAI Can Be Misused,” stating

Studies document the extent to which large collections of sensitive and intimate information about individuals, CAI or not, can be subject to abuse. Documented examples of LOVEINT abuses (government officials spying on actual or potential romantic partners) involving other intelligence collections demonstrate the potential for comparable abuse of CAI held by the IC. In the wrong hands, sensitive insights gained through CAI could facilitate blackmail, stalking, harassment, and public shaming.

Ex. 4 at 22.

24. The ODNI Report states that “the IC does not currently have sufficient visibility into its own acquisition and use of CAI across its 18 elements.” (Ex. 4 at 31). The report explains that “prior retrospective data calls have not fully succeeded. An attempt from the beginning of 2021 did not return comprehensive and reliable results, and – in part for that reason – the data call underlying our report sought only representative samples of CAI.” (Ex. 4 at 31). The report cautions that

[o]ur report is not ... based on anything approaching a complete survey of the use of CAI by the IC, and difficulties in accessing historical information about the use of CAI informs our recommendation for a new, forward-looking approach. Depending on what is revealed by that forward-looking approach, significant new work may be required. For example, as noted throughout this report, our report addresses CAI that is publicly available; if it turns out to be the case that the IC acquires and uses a significant amount of CAI that is *not* PAI (e.g., because it is sold only to governmental customers, not to the general public), then further analysis on that issue probably would be necessary.

Ex. 4 at 32.

25. The ODNI Report recommends that “The IC Should Learn How It Acquires and Uses CAI”:

First, the IC should develop a multi-layered process to catalog, to the extent feasible, the CAI that IC elements acquire. This will be a complex undertaking requiring attention to procurement contracts, functionally equivalent data acquisition processes, data flows, and data use. The IC cannot understand and improve how it deals with CAI unless and until it knows what it is doing with CAI.

Ex. 4 at 31. The report states that, with improved IC insight into its own CAI practices:

Logically inconsistent approaches to CAI (as opposed to mere differences in approach, which properly may result from differences in mission, authorities, and other factors) can be found and addressed. In addition, overseers will rightly pose questions about the IC’s approach to CAI, and the IC should be able to answer those questions with high fidelity and confidence.

Ex. 4 at 31. The report states: “our assessment is that current practices vary more, and more unsystematically, than is best. Put differently, the IC’s approach to CAI so far has been mainly federated, with individual elements operating as what might be called laboratories of CAI governance.” Ex. 4 at 33.

26. The ODNI Report states:

If the IC finds that it acquires CAI through mechanisms outside the scope of what we have described in this report, then of course those mechanisms should be examined as well. Here, as in the definition of CAI, attempts to describe a formal scope of effort should not obscure the functional focus on gaining the best possible understanding of the CAI that is actually being acquired and used by the IC.

Ex. 4 at 33.

27. The ODNI Report also recommends that “The IC Should Develop More Precise Sensitivity (VPS) Guidance for CAI.” (Ex. 4 at 37). The report states: “CAI can include sensitive information with a high volume, proportion, and sensitivity (VPS) of USPI [U.S. Person Information].” (Ex. 4 at 37). The report states: “We believe that the IC should develop guidance that refines and applies VPS standards more precisely and explicitly to CAI.” Ex. 4 at 37.

28. The ODNI Report recommends that IC elements “consider [multiple] substantive issues in developing VPS guidance for CAI,” including the following:

Traditional minimization approaches and techniques, including ability to acquire CAI via access to data at the vendor rather than ingestion of data in bulk, limits on retention, access, querying, other use, and dissemination of CAI, and possible requirements for special training of relevant personal [sic] and auditing of queries and other uses of CAI.

Ex. 4 at 38.

29. The ODNI Report states: “As of this writing, CIA is in the process of developing principles to govern the acquisition and use of commercial data.” Ex. 4 at 43. Assessing the CIA’s efforts, the report states: “Although it has made progress, particularly with respect to bulk (or bulky) collection of CAI, further progress needs to be made in developing visibility into and control of the channels through which CIA acquires CAI.” Ex. 4 at 44.

August 4, 2023

Respectfully submitted,

/s/ Gene C. Schaerr

GENE C. SCHAERR (D.C. Bar No. 416368)

Brian J. Field (D.C. Bar No. 985577)

SCHAERR | JAFFE LLP

1717 K Street NW, Suite 900

Washington, DC 20006

(202) 787-1060

gschaerr@schaerr-jaffe.com

Counsel for Plaintiff

EXHIBIT 1

From: Benjamin Huebner-DNI-
To: Bradley A. Brooker-DNI-; (b)(3), (b)(6)
Subject: limited distro, draft paper on commercially acquired information, quick turn
Date: Monday, March 1, 2021 11:02:53 PM
Attachments: [image001.jpg](#)
[CAI white paper March 2021 v.1.docx](#)

Classification: ~~TOP SECRET//SI//NOFORN~~

(b)(3)

Brad (b)(3), (b)(6)

(U//FOUO) As you know (and as I warned Brad earlier this evening), about a month ago, the DNI tasked CLPT with drafting a white paper regarding commercially acquired information – how to define it, what the advocates arguments were with regard to it, and what we thought of those arguments. The DNI requested a “1-2 page outline,” but the best I could muster is this 9 page paper. The paper is the result of CLPT’s, so far informal, discussions with the NGO community, a review of the various press articles and a recent letter from House members, as well as my own musings on how these procedures are being implemented across the IC. The paper is CLPT’s alone, and as you will see still needs some citations and a good copy edit. I need to complete it and get it to the DNI by COB tomorrow. In this case, I have purposely written this as a CLPT paper and recommendation, making no comment on the legal arguments (though references to *Carpenter* are inevitable), so not asking for OGC to endorse the paper or its findings/recommendations. But would be very interested in your thoughts.

(U//FOUO) If the DNI assesses CLPT is on the right track, a version of this paper would be the initial discussion paper for the CAI Framework group that the IC Civil Liberties and Privacy Council is setting up. As I will tell folks on Brad’s GC call, your participation and that of your legal colleagues in other IC elements will be most welcome, but we are ultimately looking to establish a policy of how the IC should handle commercially available information, as opposed to articulate the legal requirements. Easier said than done, which is why broad OGC participation is welcome.



Ben Huebner
Chief, Office of Civil Liberties, Privacy, and Transparency
(b)(3)

=====
Classification: ~~TOP SECRET//SI//NOFORN~~

EXHIBIT 2

~~TOP SECRET//SI//NOFORN~~

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

(U) Key Concepts Relevant to a Framework for the Intelligence Community's Acquisition and Use of Commercially Acquired Information

ODNI Office of Civil Liberties, Privacy, and Transparency


March 2021

(U) Executive Summary

(U/~~FOUO~~) The Intelligence Community has a common definition of publicly available information and an emerging definition of commercially available information. Because even publicly available information varies in sensitivity and commercially available information may be acquired by the IC through means other than purchase, this paper uses the term *commercially acquired information* (CAI) to describe datasets purchased by the IC through commercial means for intelligence purposes.

(U) External advocates and some Members of Congress have expressed concern that changes in technology, combined with the increasingly widespread commercial sale of detailed information related to mobile telephony use, now permit the IC to engage in near-ubiquitous surveillance through the purchase data that normally would require a court order to obtain. Advocates are most concerned about the IC's purchase and use of (1) location information, (2) communications content and other related metadata, (3) biometric data (particularly related to facial recognition), and (4) other bulk datasets (to include consumer profiles) that may allow for inferences regarding Constitutionally-protected activities (including political affiliation). Advocates seek restrictions on the bulk purchase of such information and a judicial warrant requirement for any targeted collection.

(b)(1), (b)(3)



Page 1

(b)(3)



DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

(U) Distinguishing Publicly Available Information, Commercially Available Information, and Commercially Acquired Information

(U) IC elements generally utilize the following common definition for *publicly available information*:

(U) **Publicly available** means information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer (but not amounting to physical surveillance), is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.

This definition is found in the Attorney General-approved procedures required by Executive Order 12333 Section 2.3 in order for an IC element to collect, retain, or disseminate United States person information. Some IC element EO 12333 procedures expand upon, but do not substantively modify, the above definition.

(U) IC element EO 12333 procedures favor the acquisition of publicly available information as the “least intrusive” collection technique; mandates to limit the breadth of information collected may be subordinate to the requirement to use the least intrusive collection means.¹ Privacy and civil liberties concerns related to the acquisition and use of publicly available information by an IC element may be high (publicly available social media postings by minors), low (newspaper articles regarding an individual of potential counterintelligence concern), or non-existent (published global wheat prices). While acquisition, retention, and dissemination standards for publicly available information are the most permissive, acquisition and handling of such information must still be for authorized purposes and in compliance with Constitutional and statutory constraints.

(U//~~FOUO~~) There is not a similar common definition for *commercially available information* in the IC elements’ EO 12333 procedures. The closest common definition is the more recently developed by the IC Chief Data Officers Council as part of the IC Data Management Lexicon:

¹ (U) See Executive Order 12333 § 2.4 (stating IC elements “shall use the least intrusive collection techniques feasible *within the United States or directed against United States persons abroad*”) (emphasis added). Compare Department of Defense Manual (DoDM) 5240.01 Paragraph 3.2.f.(3) (implementing EO 12333 least intrusive means requirement) with Paragraph 3.2.f.(4) (requiring Defense Intelligence Components to limit the amount of *non-publicly available* information collected, to the extent practicable, to no more information than is reasonably necessary, but subordinating this requirement to the least intrusive means requirement). See also CIA Attorney General Guidelines § 1.3(b) (restating EO 12333 least intrusive means requirement), 3.3 (limiting CIA collection to “only the amount of information reasonably necessary to support” an authorized collection purpose), 4.1 and 4.2 (implementing EO 12333 least intrusive means requirements and determining that “as a rule” collection of publicly available information is a less intrusive collection technique), and 5.1 and 5.2 (requiring for bulk and other large collections of unevaluated information, approval documentation include the “reasonable steps that were or will be taken to limit the information to the smallest separable subset of data containing the information necessary to achieve the purpose of the collection”).

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

(U) **Commercially Available Information** - Any information that is of a type customarily made available or obtainable and sold, leased, or licensed to the general public or to non-governmental entities for purposes other than governmental purposes. Commercially Available Information also includes information [data] for exclusive government use, knowingly and voluntarily provided by, procured from, or made accessible by corporate entities at the request of a government entity, or on their own initiative.

(U//~~FOUO~~) Not all commercially available information constitutes publicly available information. Data or other information sold exclusively to government entities constitutes commercially available information, but not publicly available information. This is a distinction with a significant difference as non-publicly available, commercially-available information is subject to more restrictive acquisition, retention, and dissemination controls associated with other forms of collection, such as information acquired from tasked human sources.

(U//~~FOUO~~) In addition, certain information may be commercially available, but the IC element may not acquire it through commercial means. For example, a dataset may be generally available for purchase, but an IC element may use HUMINT or SIGINT means to collect the data in order to obfuscate the U.S. government's acquisition of the data. This paper uses the term **commercially acquired information (CAI)** in order to clarify that we are only addressing those instances where an IC element has in fact acquired commercially available information through commercial means, whether or not that data is publicly available.

(b)(5)

(U) **External Critiques of the Intelligence Community's Collection and Use of CAI**

(U) Critiques of the collection and use of CAI are not limited to collection and use by IC elements, but reflect larger criticisms regarding the use of CAI by the USG writ large.² External critiques generally do not question the potential utility of CAI to meet the government's objectives, but instead take aim at the premise that publicly available information or CAI generally raises *de minimis* privacy concerns. Advocates argue that significant reforms are needed due to structural changes in the digital environment, most particularly (a) the ubiquity of smart phone-generated data, particularly data associated with the user's location, and (b) the

² See, e.g., Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, New York Times, January 22, 2021 (reporting Senator Wyden's characterization that an IC element "instead of getting an order, just goes out and purchases the private records of Americans from these sleazy and unregulated commercial data broker who are simply above the law"); [cite to November 2021 Vice Motherboard tech blog article on Muslim Pro and Quran App]; [cite to 02.18.2021 Muslim App letter from House Members]; [cite to February 18, 2021 letter to Senators Wyden and Warren from Treasury IG regarding IRS use of Venntel data]; [cite to 2020 WSJ articles on ICE and CBP use of data for border control and immigration enforcement] [cite to October 2020 BuzzFeed article DHS legal memo on smartphone location data]; [cite to February 2021 DHS article]

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

aggregation and sale of data by third party data brokers who may not be covered by existing statutory and regulatory privacy requirements. Though often couching critiques of government acquisition in legal terms, advocates have mixed opinions on whether government (or at least the IC) acquisition of such information is currently unlawful, but are generally uniform in asserting that either through statutory changes or the further development of case law related to the Supreme Court's decision in *Carpenter v. United States*³ (ideally, both) collection and use of certain categories of data should be unlawful if purchased in bulk, and legally permitted only in targeted cases after obtaining a judicial warrant.

(U) Categories of CAI of particular concern to advocates include:

- (1) **Location Information:** Virtually all conversations with advocates begin with concerns regarding the acquisition and use, particularly the bulk acquisition and use, of geo-location data. Advocates note that though *Carpenter* explicitly states that the opinion does not consider “collection techniques involving foreign affairs or national security”⁴ the logic holds that individuals protected by the Fourth Amendment have a reasonable expectation of privacy in their location independent of the government's purpose for acquiring such data. Advocates note that precise information regarding location often would reveal an individual's home and work locations, obviating any nominal anonymization of the location data. Advocates point out that location information may reveal political associations, participation in lawful protests and other freedom of speech/association-related activities, religious affiliation, and the exercise of other Constitutionally-protected rights.
- (2) **Communications Content and Other Related Metadata:** Advocates assert that third party data brokers sell data that if obtained from by the government from traditional electronic communication service providers would require a court order or other legal process. Concerns include commercially available information regarding (a) Internet search terms used by individuals; (b) web-browsing data; and (c) bulk social media content that is publicly available, but for which social media companies use privacy policies and terms of service agreements to bar the sale to the USG. Advocates view such purchases as exploiting “loopholes” in the Electronic Communications Privacy Act (ECPA) and the Stored Communications Act and raise concerns that purchase of such information could be used to impinge on privacy interests protected by the Fourth Amendment or activities protected by the First Amendment.
- (3) **Biometric Data:** Advocates concerns regarding biometric data generally fall within several subcategories. First, and related to the above concern regarding the privacy and civil liberties implications of location information, advocates raise concerns that when utilized in conjunction with other technology, bulk biometric data could be used to

³ (U) 138 S. Ct. 2206 (2018).

⁴ (U) *Id.* at 2220.

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

facilitate mass location-tracking of individuals (e.g., use of facial recognition with pervasive video surveillance of public locations). Second, advocates raise concerns that some technologies that rely upon biometrics, particularly facial recognition technology, are disproportionately inaccurate in identifying women and non-white individuals, which may result in or exacerbate disparate treatment. Third, in some instances, certain biometrics (particularly DNA) may in and of themselves convey medical information that raises privacy concerns.

(4) Other Bulk Data that May Allow for Inferences Regarding Constitutionally-Protected Activities: Some advocates note that in a rapidly changing digital environment, limiting protections to only certain categories of data would fail to protect Americans if data was collected and analyzed in bulk in a manner that allows the Government to monitor Constitutionally-protected activities. Whether it is using data from an IoT refrigerator or thermostat to monitor when an individual is located in their home or the review of consumer profiles that could reveal political or other affiliations, the concern is that the USG may engage in population-level monitoring by applying advanced analytics to the digital dust created in an IoT world.

(U) Critics of the acquisition and use of the above categories of information acknowledge that limiting the USG's acquisition and use of commercially available information may place the USG at a disadvantage relative to foreign adversaries who will continue to purchase such information, but see this as an argument for Congress to enhance restrictions on the commercial sale of such information across the board. Advocates note that ECPA has long restricted the government's acquisition of certain forms of data that are otherwise permitted to be used for other commercial purposes.

(U) Advocates also assert that a lack of transparency regarding what the government purchases stifles public debate on the appropriate role of government with respect to CAI. They also express concerns that a lack of transparency results in individuals limiting their Constitutionally-protected activities out of concerns, founded or unfounded, that the government monitors such activity through the use of CAI.

(U) Evaluation of Critiques and Proposed Scope of CAI Framework to Address Them

(U) This paper does not evaluate the validity of the legal claims made by advocates, but instead addresses some of the underlying privacy and civil liberties concerns that animate them.

(U//~~FOUO~~) The concerns raised by the advocates are not specific to the IC, or even to the USG, but reflect a societal discussion regarding the implications of mass and massive data creation through the use of smart phones and IoT devices. The advent of "Big Data," in correlation with the emergence of third party data brokers and advanced data analytics, has created a digital environment that allows for commercial monitoring of individuals at a scale and depth

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~
 DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

previously not contemplated. Society as a whole, both through national privacy legislation and international disagreements on data protections, is reconsidering and reformulating both norms and regulations as a result of this new reality.

(U//~~FOUO~~) In some respects, the IC is well positioned for this reorientation. The IC is completing a multi-year update of IC element EO 12333 procedures. The revised EO 12333 procedures strengthen controls by taking a holistic approach to privacy and civil liberties protection, to include additional approval processes, documentation, access controls, query justifications, and retention limits for data collections involving a significant volume, proportion, and/or heightened sensitivity of U.S. person information. The revised EO 12333 procedures also impose heightened privacy and civil liberties controls on CAI that is not publicly available.

(U//~~FOUO~~) These EO 12333 procedures further implement underlying Constitutional, statutory, and Executive Order protections that prohibit the IC from conducting activities that unduly impact the privacy and civil liberties of United States persons. All intelligence activities, to include collection, querying, use, and dissemination may be undertaken only for an authorized intelligence purpose. IC elements are prohibited from collecting or maintaining information concerning U.S. persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States.⁵ IC elements are also barred from engaging in any intelligence activity for the purpose of affecting the political process in the United States.⁶

(U//~~FOUO~~) Despite these protections, CLPT assesses that additional guidance regarding the application of the EO 12333 procedures to commercially available information is needed for the following reasons:

(U//~~FOUO~~) First, the above-stated protections may be found in the IC elements' publicly-released EO 12333 procedures, but these protections are embedded in detailed legal documents that are available, but not necessarily functionally accessible, to the public. In some instances, controls are spread over multiple sections and fully understood only through the correlation of several cross-references.⁷ While some IC elements have released plain language explanatory documents regarding their U.S. person protections,⁸ there is no DNI-issued guidance that clearly and authoritatively articulates the basic protections common to all of the EO 12333 procedures.⁹

(U//~~FOUO~~) Second, the complexity of the EO 12333 procedures, combined with the intended flexibility for certain publicly available information of limited privacy and civil liberties concern,

⁵ (U//~~FOUO~~) See, e.g., CIA Executive Order 12222 procedures at Section 3.3.

⁶ (U//~~FOUO~~) See, e.g., DoDM 5240.01 at Paragraph 3.1.a.(4).

⁷ (U) See, e.g., *supra* footnote 1.

⁸ (U//~~FOUO~~) See CIA Narrative Summary. See ODNI Release Statement

⁹ (U//~~FOU~~) ODNI has previously released *Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publicly Available Information*, but this 2011 guidance predates the modern revisions to the EO 12333 procedures and is guidance issued by the Civil Liberties Protection Officer, not the DNI. Available at [\[insert link.\]](#)

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

could lead to unintended results. For example, CIA's EO 12333 procedures require approval and documentation for large data acquisitions and require approval and documentation of the steps taken to limit collection or retention to the smallest separable subset of data containing the information necessary to achieve the purpose of the collection.¹⁰ Although more restrictive handling procedures are required for datasets of unevaluated information that contain U.S. person identifying information that is significant in volume, proportion, or sensitivity (hereinafter "VPS data"),¹¹ such protections are not required for data that has been determined to qualify for retention in its entirety,¹² and one of the criteria permitting such retention is that the U.S. person information is publicly available.¹³ This leads to the sensible result that more restrictive handling requirements are not required for newspaper articles (which may have a high proportion or volume of U.S. person information), but could also in theory result in the determination that a broad dataset of U.S. person location information that is commercially available does not require the highest level of privacy and civil liberties controls. A clear, IC-wide CAI framework would ensure that both the public and IC elements read the applicable EO 12333 procedures as a whole and in a manner that does not lead to unintended results.

(U//~~FOUO~~) Relatedly, while additional protections are required for VPS data, there is no IC-wide guidance and limited IC element guidance regarding the types of collections that would meet the volume, proportion, or sensitivity standards that trigger these heightened requirements. While application of the "volume" and "proportion" aspects of the VPS test may be largely contextual and require the exercise of judgment, further guidance could clarify that certain categories of data concerning United States persons are *per se* sensitive enough to trigger requirements for heightened approvals and more restrictive controls even if the data has been purchased commercially or is publicly available. Several of the categories identified by advocates – specific and persistent location information of U.S. persons, bulk social media content, and data used for biometric purposes – all could reasonably qualify as inherently sensitive datasets even if commercially acquired or drawn from publicly available information. While the advocates' preference for a judicial warrant requirement for obtaining such information would be burdensome, the application of the heightened approval and handling requirements associated with VPS data would help ensure such collection is restricted to that which is necessary to support the IC's mission and that the resulting data is appropriately handled constituent with respect for privacy and civil liberties concerns.

(U//~~FOUO~~) Third and finally, the development of the CAI framework should consider whether to prohibit or substantially restrict, as a matter of policy, the bulk collection of persistent mobile location information of individuals located in the United States. Bulk purchase and use of such

¹⁰ (U//~~FOUO~~) See CIA EO 12333 Guidelines at Section 5.

¹¹ (U//~~FOUO~~) See CIA EO 12333 Guidelines at Section 6.2.1(b).

¹² (U//~~FOUO~~) See CIA EO 12333 Guidelines at Section 6.1(c).

¹³ (U//~~FOUO~~) See CIA EO 12333 Guidelines at Section 7(b). Similarly, DoD EO 12333 procedures require special approvals to collect VPS data and the consideration of the appropriate enhanced safeguards, *see, e.g.,* DoDM 5240.01 at Paragraph 3.2.e., but require only that the collection of "non-publicly available" United States person information" be limited to that which is "reasonably necessary." *See, e.g.,* DoDM 5240.01 at Paragraph 3.2.f.(4).

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

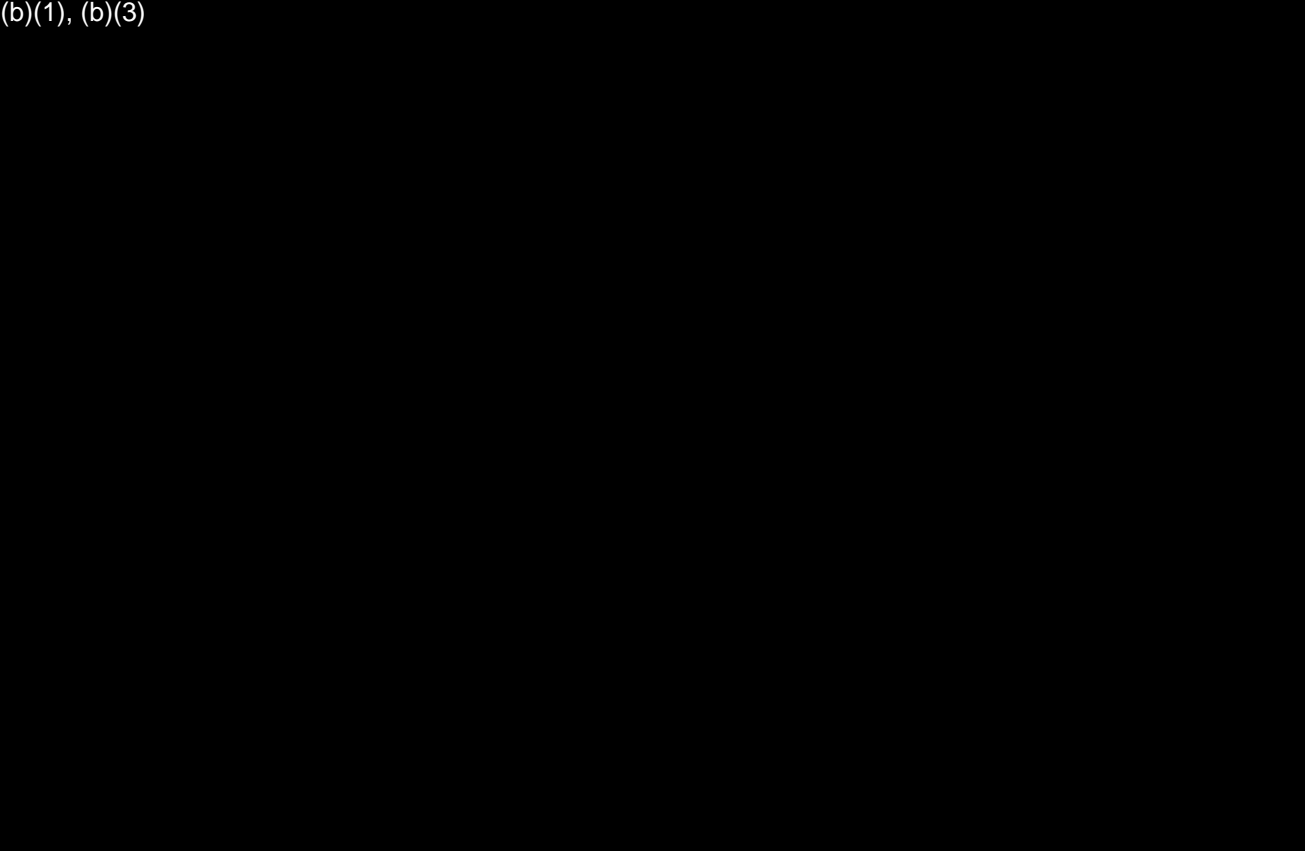
~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

information currently presents the most significant privacy and civil liberties concerns. The capability to monitor, historically and persistently, the American populace at scale was likely unimaginable to the Founders. While the *Carpenter* decision explicitly did not consider national security matters, due to the “unique nature of cell phone location records,” the Supreme Court declined to extend the third-party doctrine to such data,¹⁴ noting that “[m]aping a cell phone’s location over the course of 127 days provides an all-encompassing records of the holder’s whereabouts” revealing “not only his particular movements, but through them his familial, political, professional, religious, and sexual associations.”¹⁵ The prevalence of cell phones, combined with the commonality of location-tracking mobile applications, severely limits the ability of individuals to opt-out of such ubiquitous surveillance. While many commercially available datasets of location information are purportedly anonymized, the ability to track a cell phone persistently allows such information to be deanonymized with few additional data points,¹⁶ and presumably the purpose of the IC acquiring such information would often be to identify a specific individual and track their associations and movements.

(b)(1), (b)(3)



¹⁴ 138 S. Ct. at 2217.

¹⁵ *Id.* (internal quotation removed)

¹⁶ Cite to December 2019 NYTimes series.

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~
DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

(U//~~FOUO~~) We should not expect that any enhancement or clarification of the IC's internal controls for CAI will fully satisfy advocates, as advocates seek to impose external controls (statutory and case law) to bind the IC and prevent classified exceptions or reinterpretations of existing policy. Such external restrictions may have significant unintended consequences. The IC, however, can assure the public that it is properly and appropriately collecting and handling CAI by clearly and publicly articulating our common framework for CAI, clarifying that collection/retention/dissemination protections apply for VPS data even when such data is publically available, and establishing a baseline across the IC for certain types of data requiring enhanced safeguards. The IC should also evaluate its purchase and use of bulk location information within the United States and determine whether to prohibit or substantially restrict the purchase and use of such information for mission purposes.

DELIBERATIVE PROCESS PRIVILEGED DOCUMENT

~~TOP SECRET//SI//NOFORN~~

EXHIBIT 3

ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 4 PAGES 4

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER 09/13/2017		2. CONTRACT NO. (If any) DJF-17-1200-P-0007190		6. SHIP TO:	
3. ORDER NO. DJF-17-1200-P-0007190		4. REQUISITION/REFERENCE NO. DJF-17-1600-PR-0005216		a. NAME OF CONSIGNEE SEE SCHEDULE	
5. ISSUING OFFICE (Address correspondence to) FEDERAL BUREAU OF INVESTIGATION INFORMATION TECHNOLOGY CONTRACTS UNIT 935 PENNSYLVANIA AVE, NW WASHINGTON, DC 20535-0001				b. STREET ADDRESS	
7. TO: a. NAME OF CONTRACTOR ARGONNE RIDGE GROUP, LLC		c. CITY		d. STATE	e. ZIP CODE
b. COMPANY NAME		f. SHIP VIA			
c. STREET ADDRESS 901 INTL PKWY STE 350		DUNS: 785086948		8. TYPE OF ORDER	
d. CITY LAKE MARY		e. STATE FL	f. ZIP CODE 32746-4799	<input type="checkbox"/> a. PURCHASE <input type="checkbox"/> b. DELIVERY -- Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.	
9. ACCOUNTING AND APPROPRIATION DATA FBI-2017-SEN1-1600-1600-OT-OT-25103-COMP-2017				10. REQUISITIONING OFFICE CYBER DIV ATTN: [REDACTED] M-RIDG A CYD 2400 SCHUSTER DRIVE CHEVERLY, MD 20781-0001	
11. BUSINESS CLASSIFICATION (Check appropriate box(es)) <input checked="" type="checkbox"/> a. SMALL <input type="checkbox"/> b. OTHER THAN SMALL <input type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED <input type="checkbox"/> e. HUBZone <input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED <input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM <input type="checkbox"/> h. EDWOSB				12. F.O.B. POINT	
13. PLACE OF		14. GOVERNMENT B/L NO.		15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	
a. INSPECTION	b. ACCEPTANCE			NET 30	

b6
b7C
b7E

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
0001	Firm Fixed Price Commercially provided net flow information/data - 2 months of service PSC: D302 See Continuation Sheet(s)	1	EA	\$76,450.0000 Fees: \$0.00	\$76,450.00	

SEE BILLING INSTRUCTIONS ON REVERSE	18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		\$76,450.00	17(h) TOT. (Cont. pages)
	21. MAIL INVOICE TO:							
	a. NAME CYBER DIV Attn: [REDACTED]						\$76,450.00	17(i) GRAND TOTAL
	b. STREET ADDRESS (or P.O. Box) ATTN: [REDACTED] M-RIDG A CYD, 2400 SCHUSTER DRIVE							
c. CITY CHEVERLY		d. STATE MD	e. ZIP CODE 20781-0001					
22. UNITED STATES OF AMERICA BY (Signature)						23. NAME (Typed) (D)Laurie L. Williams TITLE: CONTRACTING/ORDERING OFFICER		

b6
b7C

Section 2 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
	Line Period of Performance: 09/15/2017 - 11/15/2017 Base Period Delivery Schedule: Quantity: 1.000000 FOB: Delivery Address: CYBER DIV ATTN: [REDACTED] M-RIDG A CYD 2400 SCHUSTER DRIVE CHEVERLY, MD 20781-0001			\$76,450.0000	\$76,450.00
Base Total:					\$76,450.00
Exercised Options Total:					\$0.00
Unexercised Options Total:					\$0.00
Base and Options Total:					\$76,450.00

b6
b7c

FUNDING DETAILS:

ITEM NO.	FUNDING LINE	OBLIGATED AMOUNT	ACCOUNTING CODES
0001	1	\$76,450.00	FBI-2017-SEN1-1600-1600-OT-OT-25103-COMP-2017
		TOTAL: \$76,450.00	

Section 3 - Contract Clauses

This Section Is Intentionally Left Blank

Section 4 - List of Attachments

This Section Is Intentionally Left Blank

EXHIBIT 4

~~SECRET~~ // [REDACTED]

(U) Office of the Director of National
Intelligence
Senior Advisory Group
Panel on Commercially Available Information

(U) Report to the Director of National Intelligence
27 January 2022

Classified By: [REDACTED]
Derived From: [REDACTED]
Declassify On: [REDACTED]

~~SECRET~~ // [REDACTED]

~~SECRET~~ // [REDACTED]

~~SECRET~~ // [REDACTED]

~~SECRET~~ / [REDACTED]

27 January 2022

The Honorable Avril Haines
Director of National Intelligence
Washington, DC 20511

Dear DNI Haines:

(U) With this letter, we transmit our 90-day report on commercially available information (CAI). We appreciate your commissioning the report and the assistance of your office and other Intelligence Community (IC) elements in this time-sensitive undertaking.

(U) As prescribed in our terms of reference (TOR), the report attempts to “(1) describe the role of CAI in intelligence collection and analysis; (2) reflect on the existing framework for ensuring the protection of privacy and civil liberties; and (3) make[] recommendations to the IC regarding how and under what circumstances an IC element should collect, use, retain, and disseminate CAI.” These three issues, preceded by a background description and explanation of CAI, are addressed in the four main parts of our report.

(U) Our report does not attempt “an independent legal analysis” of the issues involved with CAI, as set forth in our TOR, but instead follows the IC’s own approach in considering questions of CAI policy.

(U) Our report addresses CAI that is available for purchase by the general public and as such is treated as a subset of publicly available information (PAI). Unless otherwise indicated in context, we use the term “CAI” in this report to refer to CAI that is also PAI.

(U) Highlights of our report include the following:

1. (U) There is today a large and growing amount of CAI that is available to the general public, including foreign governments (and their intelligence services) and private-sector entities, as well as the IC.
2. (U) CAI clearly provides intelligence value, whether considered in isolation and/or in combination with other information, and whether reviewed by humans and/or by machines. It also raises significant issues related to privacy and civil liberties. The widespread availability of CAI regarding the activities of large numbers of individuals is a relatively new, rapidly growing, and increasingly significant part of the information environment in which the IC must function.

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

3. (U) Under IC elements' rules and procedures, CAI (because it is also PAI) is less strictly regulated than other forms of information acquired by the IC. In our view, however, profound changes in the scope and sensitivity of CAI have overtaken traditional understandings, at least as a matter of policy. Today's publicly available CAI is very different in degree and in kind from traditional PAI.

4. (U) We have three recommendations concerning the acquisition and treatment of CAI by the IC.

(U) First, the IC should develop a multi-layered process to catalog, to the extent feasible, the CAI that IC elements acquire. This will be a complex undertaking requiring attention to procurement contracts, functionally equivalent data acquisition processes, data flows, and data use. The IC cannot understand and improve how it deals with CAI unless and until it knows what it is doing with CAI.

(U) Second, based on the knowledge gained from that process, the IC should develop a set of standards and procedures for CAI, governing and requiring regular re-evaluation of acquisition and use decisions, including as to the use of CAI. We offer several points that can be included in those standards and procedures, but also recognize that they will need to be adapted for different IC elements with different CAI needs and missions.

(U) Third, as part of this set of policies and procedures, and/or as a complement to it, the IC should develop more precise guidance to identify and protect sensitive CAI that implicates privacy and civil liberties concerns. Again, we offer several suggestions for the development of such guidance.

(U) The single most important point in our report is this: CAI is increasingly powerful for intelligence and increasingly sensitive for individual privacy and civil liberties, and the IC therefore needs to develop more refined policies to govern its acquisition and treatment. Our report does not prescribe those policies (in keeping with our timeline and role as outside advisors) but we hope that it will assist the IC with their development.

(U) We appreciate the opportunity to be of service.

Respectfully submitted,

[REDACTED]

~~SECRET~~ / [REDACTED]

~~SECRET~~ // [REDACTED]

~~SECRET~~ // [REDACTED]

~~—SECRET—~~ / [REDACTED]**(U) TABLE OF CONTENTS****(U) Executive Summary****1. (U) Background on CAI**

- 1.1. (U) What is CAI?
- 1.2. (U) CAI Sellers
- 1.3. (U) Examples of CAI
- 1.4. (U) Origins & Evolution of CAI
- 1.5. (U) Commercial Value of CAI
- 1.6. (U) Deanonymization/Reidentification

2. (U) The Role of CAI in Intelligence Collection and Analysis

- 2.1. (U) CAI as a Source for OSINT
- 2.2. (U) Examples of CAI Contracts
- 2.3. (U) Examples of CAI Value
- 2.4. (U) Non-Analytic Uses of CAI
- 2.5. (U) Counter-Intelligence Risks in CAI
- 2.6. (U) Sensitivity of CAI
 - 2.6.1. (U) CAI Includes Sensitive and Intimate Information
 - 2.6.2. (U) Defining Sensitivity Categorically
 - 2.6.3. (U) CAI Can Be Misused
 - 2.6.4. (U) CAI Increases the Power of the Government
 - 2.6.5. (U) Aggregation of CAI Raise the Risk of Mission Creep
 - 2.6.6. (U) Public, Media, and Political Scrutiny
 - 2.6.7. (U) Need for Thoughtful Approach
- 2.7. (U) Summary

3. (U) The Existing Policy Framework For CAI

- 3.1. (U) PAI
 - 3.1.1. (U) Constitutional Provisions
 - 3.1.2. (U) Federal Statutes
 - 3.1.3. (U) Pending Legislation
 - 3.1.4. (U) IC Policy
 - 3.1.5. (U) IC Guidance
- 3.2. (U) CAI
- 3.3. (U) CAI Under IC Guidelines
 - 3.3.1. (U) Authorized Purpose
 - 3.3.2. (U) Publicly Available

~~—SECRET—~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

3.3.3. (U) Scope of Collection

3.3.3.1. (U) Clarification of Current Guidelines

3.3.4. (U) Volume, Proportion, Sensitivity (VPS) of USPI

3.4. (U) CAI & Carpenter

4. (U) Recommendations

4.1. (U) Recommendation #1: The IC Should Learn How It Acquires and Uses CAI

4.1.1. (U) The Value of Understanding

4.1.2. (U) Prospective Cataloguing Effort

4.1.3. (U) Multi-Layered Cataloguing Effort

4.1.4. (U) Common Taxonomy and Understanding

4.2. (U) Recommendation #2: The IC Should Develop a Set of Adaptable Standards and

(U) Procedures for CAI

4.2.1. (U) Issues

4.2.2. (U) Examples of Current CAI Approaches

4.2.2.1. (U) Treasury

4.2.2.2. (U) Department of Homeland Security (DHS)

4.2.2.3. (U) [REDACTED]

4.2.3. (U) Assessment of CAI Examples

4.3. (U) Recommendation #3: The IC Should Develop More Precise Sensitivity (VPS)

Guidance for CAI

4.3.1. (U) Structural and Procedural Issues

4.3.2. (U) Substantive Issues

4.3.3. (U) Examples of VPS Guidance

4.3.3.1. (U) DIA

4.3.3.2. (U) NSA

4.3.3.3. (U) CIA

4.3.4. (U) Assessment of VPS Examples and Possible Areas of Future Focus

5. (U) Conclusion

6. (U) Appendices

6.1. (U) Letter and Terms of Reference

6.2. (U) IC Elements' Materials Governing CAI

6.3. (U) IC Elements' Materials on VPS and/or CAI Collection

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]**(U) EXECUTIVE SUMMARY**

(U) There is today a large and growing amount of what the U.S. Intelligence Community (IC) refers to as “Commercially Available Information” (CAI). As the acronym indicates, and as we use the term in this report, CAI is information that is available commercially to the general public, and as such, is a subset of publicly available information (PAI). We do not use the term CAI to include, and we do not address in this report, commercial information that is available exclusively to governments. The volume and sensitivity of CAI have expanded in recent years mainly due to the advancement of digital technology, including location-tracking and other features of smartphones and other electronic devices, and the advertising-based monetization models that underlie many commercial offerings available on the Internet. Although CAI may be “anonymized,” it is often possible (using other CAI) to deanonymize and identify individuals, including U.S. persons.

(U//~~FOUO~~) CAI clearly provides intelligence value, whether considered in isolation and/or in combination with other information, and whether reviewed by humans and/or by machines. The IC currently acquires a significant amount of CAI for mission-related purposes, including in some cases social media data [REDACTED] and many other types of information. As a resource available to the general public, including adversaries, CAI also raises counter-intelligence risks for the IC. It also has increasingly important risks and implications for U.S. person privacy and civil liberties, as CAI can reveal sensitive and intimate information about individuals. Without proper controls, CAI can be misused to cause substantial harm, embarrassment, and inconvenience to U.S. persons. The widespread availability of CAI regarding the activities of large numbers of individuals is a relatively new, rapidly growing, and increasingly significant part of the information environment in which the IC must function. That is the core of why it was necessary and appropriate for the IC to recognize the complex issues inherent in modern CAI and to commission this report.

(U//~~FOUO~~) Under the U.S. Constitution, federal statutes, and IC elements’ internal procedures, CAI is generally less strictly regulated than other forms of information acquired by the IC, principally because it is publicly available. In our view, however, changes in CAI have considerably undermined the historical policy rationale for treating PAI categorically as non-sensitive information, that the IC can use without significantly affecting the privacy and civil liberties of U.S. persons. For example, under [Carpenter v. United States](#), acquisition of persistent location information (and perhaps other detailed information) concerning one person by law enforcement from communications providers is a Fourth Amendment “search” that generally requires probable cause. However, the same type of information on millions of Americans is openly for sale to the general public. As such, IC policies treat the information as PAI and IC elements can purchase it. While IC policies regulate such information based on the volume, proportion and sensitivity of USPI it contains, those policies may not accord sufficient

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

protection to information that is now broadly understood to be sensitive. It is not sufficient as a matter of policy simply to say that CAI is PAI; and saying so without more may be affirmatively confusing to intelligence professionals.

(U) We have three recommendations.

(U//~~FOUO~~) **First**, the IC should develop a multi-layered approach to **catalog, to the extent feasible, the acquisition and use of CAI across its 18 elements**. This cataloging process will be complex and should include formal contracts and procurement decisions, as well as functionally equivalent agency-specific data acquisition processes, because these will help identify CAI when it first arrives at (or becomes available to) an IC element. But the process also should include detection efforts at later stages of the information lifecycle, including in the process of planning for and initially using data. In particular, key inputs to the process may include (1) documentation reflecting the purchase, license, or other acquisition of a CAI dataset; (2) audits by chief information officers (CIOs) and chief data officers (CDOs) responsible for monitoring data flows across agency systems and repositories; and (3) [REDACTED]

[REDACTED] We recommend this multi-layered approach because prior retrospective efforts focused on procurement have not been successful, and because the dynamic nature of the CAI environment will require ongoing review. This first recommendation is foundational for our remaining two recommendations.

(U//~~FOUO~~) **Second**, as it gains knowledge into its own use of CAI, the IC should **develop a set of standards and procedures for CAI**, governing and requiring regular re-evaluation of acquisition and other decisions. This can be done centrally, for the IC or the Defense Intelligence Enterprise (DIE) as a whole, and/or at individual IC elements (where the approaches could vary from one element to another as long as they are consistent in principle). Either way, as the IC develops approaches to CAI, it will need to keep in mind IC elements' authorities and needs. Among the issues that should be considered in developing IC standards and procedures are the following: Mission analysis to identify need/value; Fit between mission and CAI data set, Proposed use; Vendor and data quality; Acquisition mechanics; Data security; Sensitivity and legal review; Auditing use of CAI; Periodic re-evaluation; and Other structural and procedural issues. We review several examples of IC elements' approaches to these issues, including the [REDACTED]

(U//~~FOUO~~) **Third**, as part of this set of standards and procedures, and/or as a complement to it, the IC should **develop more precise sensitivity and privacy-protecting guidance for CAI**. PAI is no longer a good proxy for non-sensitive information. Today, in a way that far fewer Americans seem to understand, and even fewer of them can avoid, CAI includes information on nearly everyone that is of a type and level of sensitivity that historically could have been obtained, if at

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

all, only through targeted (and predicated) collection, and that could be used to cause harm to an individual's reputation, emotional well-being, or physical safety. The IC therefore needs to develop more refined approaches to CAI. Among the structural and procedural issues that should be considered in developing such approaches are the following: Required involvement of relevant parties at all stages; VPS assessments generally being made prior to acquisition, or at least prior to analytic use of CAI, and ideally integrated or coordinated with CAI acquisition reviews discussed in Recommendation #2; Approval requirements, with higher levels of approval required for more sensitive cases; Documentation, retention, and availability to relevant personnel of assessments, approvals, and mitigation measures adopted; Re-evaluation of VPS assessments and measures; Forwarding of assessments and other documentation to ODNI and/or other central authorities, with a formal mechanism for periodic review to allow comparisons and discussion of best practices across IC elements and related purposes.

(U//~~FOUO~~) Apart from the structural and procedural issues above, we recommend that IC elements also consider the following substantive issues in developing VPS guidance for CAI: Sensitivity of the CAI, in keeping with the discussion of sensitivity in Part 2 of this report; Deanonymization/reidentification issues; Importance of mission served by CAI (to balance against sensitivity of CAI); Strength of nexus between CAI and mission, and availability, feasibility, costs, and risks of alternatives; Ability to filter USPI prior to ingestion; Traditional minimization approaches and techniques; Availability of other privacy-protective measures in light of the need and anticipated use of CAI.

(U//~~FOUO~~) Some IC elements have already made progress towards developing new VPS guidance, and we review several specific approaches that are in effect or are in the process of being developed. We offer four specific areas, drawn from the longer list above, in which such development would be particularly helpful. First, distinctions between types of CAI, including between historical CAI (e.g., newspapers) that are generally less sensitive, and newer forms of CAI that are generally more sensitive. Second, quantitative issues, because CAI that is acquired in bulk will almost always be more sensitive than CAI in smaller data sets. Third, special protections for USPs and USPI. Fourth and finally, issues raised by CAI that can easily be deanonymized, including implications for the definition of USPI as applied in this context.

(U) In **conclusion**, if some or all of our recommendations are agreeable, the IC will need a mechanism for putting them into effect – e.g., a traditional working group of IC senior officials. Such a working group might decide to proceed within the framework of our three recommendations, or it might adopt and build on their substance within a different framework – e.g., substantive principles; tools and procedures; and processes and approval requirements. We hope that our 90-day report provides a helpful foundation for developing more refined approaches, we believe that continued efforts will be necessary, and we appreciate the opportunity to be of service.

~~SECRET~~ / [REDACTED]

~~SECRET~~ / / [REDACTED]

1. (U) BACKGROUND ON COMMERCIALLY AVAILABLE INFORMATION

(U) There is today a large and growing amount of what the U.S. Intelligence Community (IC) refers to as “Commercially Available Information” (CAI). As the acronym indicates, and as we use the term in this report, CAI is information that is available commercially to the general public, and as such, is a subset of publicly available information (PAI). We do not use the term CAI to include, and we do not address in this report, commercial information that is available exclusively to governments. The volume and sensitivity of CAI have expanded in recent years mainly due to the advancement of digital technology, including location-tracking and other features of smartphones and other electronic devices, and the advertising-based monetization models that underlie many commercial offerings available on the Internet. Although CAI may be “anonymized,” it is often possible (using other CAI) to deanonymize and identify individuals, including U.S. persons.

1.1. (U) What is CAI? One of the challenges faced by the IC in dealing with CAI is defining the term, and hence the scope of any new guidance or policies that may be developed to address it. As the acronym indicates, and as we use it in this report, “CAI” is information that is available commercially, through a commercial transaction with another party. The acquisition may occur on a one-time or subscription basis, and may involve the IC directly ingesting the CAI or obtaining a license agreement that affords a continuing right of access. CAI typically is acquired for a fee, but as we use the term it also includes information offered at no cost if it is the type of information that is normally offered for sale – e.g., a free trial offering of CAI.

(U) As we use the term in this report, CAI does not include information that is stolen or otherwise misappropriated and then acquired from a black market or otherwise via traditional HUMINT acquisition methods (e.g., espionage). Nor does it include information obtained through traditional SIGINT acquisition methods (e.g., wiretapping) that does not involve a commercial transaction at all. As such, it does not necessarily include all information acquired from commercial entities, such as information acquired via lawful process (e.g., a search warrant or subpoena) served on a communications service provider or financial institution.

(U) In taking this approach to CAI, we generally follow the definition in the Intelligence Community Data Management Lexicon:

(U) Any information that is of a type customarily made available or obtainable and sold, leased, or licensed to the general public or to non-governmental entities for purposes other than governmental purposes. Commercially Available Information also includes information for exclusive government use, knowingly and voluntarily provided by, procured from, or made accessible by corporate entities at the request of a government entity, or on their own initiative.

~~SECRET~~ / / [REDACTED]

~~SECRET~~ / [REDACTED]

(U) Although some CAI is available only to governments, as the Lexicon notes, we use the term to mean, and this report addresses, only the subset of CAI that is generally available and is therefore also publicly available information (PAI). Under IC guidelines, PAI is defined as

information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer (but not amounting to physical surveillance), is made available at a meeting open to the public, or is observed by visiting any place or attending any event that is open to the public.

(U) Office of the Director of National Intelligence, Intelligence Activities Procedures Approved by the Attorney General Pursuant to Executive Order 12333 ([ODNI Guidelines](#)) § 10.17 (emphasis added); see also Central Intelligence Agency Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333 (CIA Guidelines) § 12.20; DOD Manual 5240.01: Procedures Governing the Conduct of DOD Intelligence Activities ([DOD Manual](#)) § G.2 at page 53.

(U) To repeat for emphasis and clarity, unless otherwise indicated in context, we use the term “CAI” to refer to CAI that is also PAI, and our report addresses only CAI that is also PAI. Non-public CAI raises distinct legal and policy questions and is beyond the scope of our current efforts.

~~(U//FOUO)~~ Our discussions with IC elements included a heavy emphasis on defining CAI, a valuable and foundational effort for this report and any future regulation of CAI. Focus on a formal definition, however, should not obscure the functional perspective that animates our recommendations. As discussed in the balance of this report, CAI merits special attention today because of its increasing importance for intelligence as well as for privacy and civil liberties (as discussed in Part 2), and because it has, at least in part, overtaken current IC policies that address it (as discussed in Part 3). Those concerns should inform efforts to apply, and if necessary to modify, the formal definition of CAI in the many, varied and evolving contexts that the IC does and will face. Cf. Privacy and Civil Liberties Oversight Board, [Report to the President on Implementation of Presidential Policy Directive 28: Signals Intelligence Activities](#) at 12, 24 (noting the absence of a formal definition of “signals intelligence” under PPD-28).

1.2. (U) CAI Sellers. A key feature of CAI is that it is often sold or otherwise made available by commercial entities. Sellers of CAI are often referred to as “data brokers” or “information resellers.” As the Government Accountability Office (GAO) [reported](#) in December 2013, these sellers of CAI

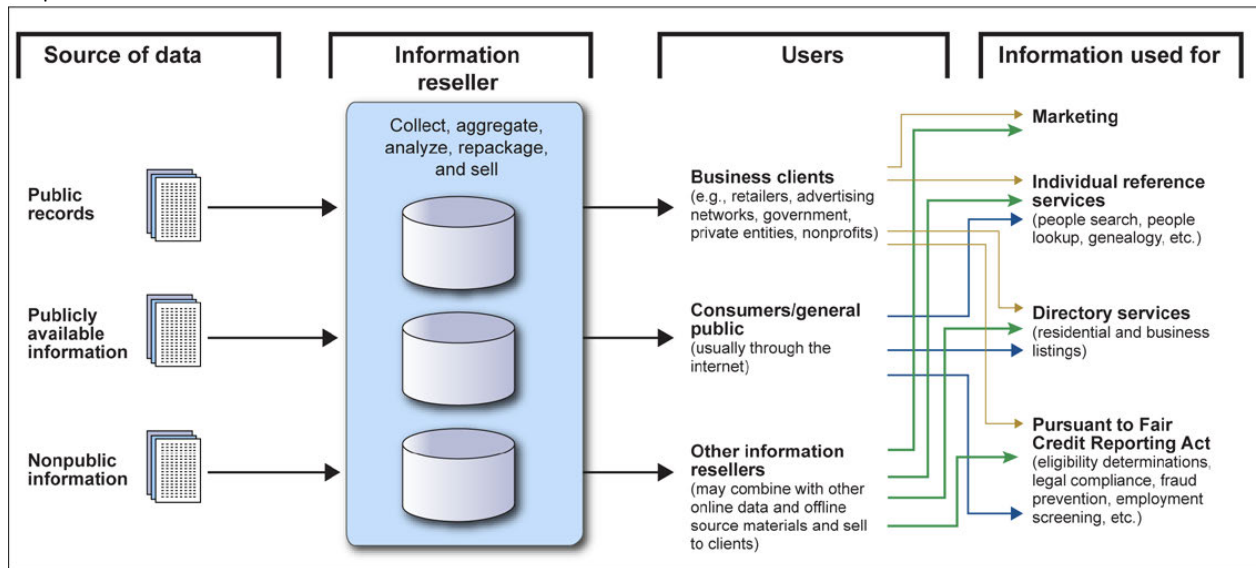
~~SECRET~~ / [REDACTED]

~~SECRET~~ // [REDACTED]

maintain large, sophisticated databases with consumer information that can include credit histories, insurance claims, criminal records, employment histories, incomes, ethnicities, purchase histories, and interests. Resellers largely obtain their information from public records, publicly available information (such as directories and newspapers), and nonpublic information (such as from retail loyalty cards, warranty registrations, contests, and web browsing). Characterizing the precise size and nature of the reseller industry can be difficult because of limited publicly known information about the industry.

(U) In [testimony](#) before the Senate Banking Committee in June 2019, a GAO official repeated the substance of those observations from 2013 and provided the following graphic to illustrate the development of and market for CAI:

Graph is Unclassified



Source: GAO. | GAO-19-621T

(U) A May 2014 [report](#) from the Federal Trade Commission (FTC) provides a similar account:

(U) Data brokers collect data from commercial, government, and other publicly available sources. Data collected could include bankruptcy information, voting registration, consumer purchase data, web browsing activities, warranty registrations, and other details of consumers’ everyday interactions. Data brokers do not obtain this data directly from consumers, and consumers are thus largely unaware that data brokers are collecting and using this information. While each data broker source may provide only a few data elements about a consumer’s activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer’s life.

(U) Civil society groups in the United States have also described data brokers and the market for CAI in the context of their public advocacy efforts. A recent example is the report from the

~~SECRET~~ // [REDACTED]

~~SECRET~~ / [REDACTED]

Center for Democracy and Technology (CDT), [Legal Loopholes and Data for Dollars](#), released in December 2021. As of this writing, major data brokers include [Accenture](#), [Axiom](#), [CoreLogic](#), [Epsilon](#), [Intelius](#), [LexisNexis](#), [Oracle](#) (Datalogix), [Thomson Reuters](#), and [Verisk](#) (these companies, and the ones further discussed below, are listed solely for purposes of illustration, and references to the work of civil society groups are similarly for descriptive purposes only). In general, CAI sellers include those focused on marketing and advertising, fraud detection, risk mitigation, and identity resolution (people finders). Purchasers of CAI include other data brokers, various private-sector and non-governmental entities, and governments worldwide, including the IC.

1.3. (U) Examples of CAI. We do not attempt a comprehensive description of the scope and scale of data that are available as CAI, or the relevant markets, in part because they are so large and so dynamic. However, a few examples of CAI offerings will illustrate the current nature of available offerings:

- (U) “Thomson Reuters [CLEAR](#)® is powered by billions of data points and leverages cutting-edge public records technology to bring all key content together in a customizable dashboard.”
- (U) [LexisNexis](#) offers more than “84B records from 10,000+ sources, including alternative data that helps surface more of the 63M unbanked/underbanked U.S. adults.”
- (U) [Exactis](#) has “over 3.5 billion records (updated monthly)” in its “universal data warehouse.”
- (U) [PeekYou](#) “collects and combines scattered content from social sites, news sources, homepages, and blog platforms to present comprehensive online identities.”

(U) As these examples show, there is a large and growing amount of CAI in existence and offered for sale, some of it sensitive with respect to privacy. The market for CAI, including analysis and exploitation of CAI for insight, is evolving both qualitatively (e.g., as to types of data available) and quantitatively (as to amounts of data available) – see, for example, this March 2021 [summary](#) from Gartner. It includes significant information on U.S. persons, much of which can be acquired in bulk. As discussed below, moreover, certain CAI that is “anonymized” and available in bulk can readily be reidentified to reveal information about individuals.

1.4. (U) Origins & Evolution of CAI. In substantial part, the vast and growing amount of available CAI results from evolving digital technology, and the proliferation of digital dust created by individuals in their daily lives. As our TOR explain, “[t]he digital revolution has placed an incredible amount of information into the hands of private actors, many of whom seek to sell the data.” For example, CAI can be obtained from public records, sometimes digitized from

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

paper originals, such as information about real estate transactions that can be found in local title offices or courthouses. It can be obtained from smartphone and other software applications, often in the form of software development kits ([SDK](#)), that collect information from devices in the U.S. and abroad. And CAI can be obtained from [cookies](#) and other methods, sometimes associated with real-time bidding ([RTB](#)) for sales of online advertising, that track end users as they browse the Internet. In April 2021, a bipartisan group of U.S. Senators raised [questions](#) about “the sharing of Americans’ data through ‘real time bidding’ – the auction process used to place many targeted digital advertisements.” The details of these digital developments are beyond the scope of this report; it is sufficient for our purposes, and widely understood among intelligence professionals and policymakers, that they have significantly contributed to the profound increase in CAI.

1.5. (U) Commercial Value of CAI. Various forms of CAI can be combined to synergistic effect in service of various commercial interests. For example, according to an October 2020 [press release](#) from Gartner, the “internet of behaviors (IoB) is emerging as many technologies capture and use the ‘digital dust’ of peoples’ daily lives. The IoB combines existing technologies that focus on the individual directly – facial recognition, location tracking and big data for example – and connects the resulting data to associated behavioral events, such as cash purchases or device usage.” As the FTC explained in its May 2014 [report](#):

(U) Data brokers rely on websites with registration features and cookies to find consumers online and target Internet advertisements to them based on their offline activities. Once a data broker locates a consumer online and places a cookie on the consumer’s browser, the data broker’s client can advertise to that consumer across the Internet for as long as the cookie stays on the consumer’s browser. Consumers may not be aware that data brokers are providing companies with products to allow them to advertise to consumers online based on their offline activities. Some data brokers are using similar technology to serve targeted advertisements to consumers on mobile devices.

(U) The commercial value of CAI is plainly high, which is why the market for CAI is large and growing.

1.6 (U) Deanonimization/Reidentification. CAI can also be combined, or used with other non-CAI data, to reverse engineer identities or deanonymize various forms of information. As the *New York Times* [reported](#) in December 2019, “[i]f you own a mobile phone, its every move is logged and tracked by dozens of companies ... The Times Privacy Project obtained a dataset with more than 50 billion location pings from the phones of more than 12 million people in this country. It was a random sample from 2016 and 2017, but it took only minutes — with assistance from publicly available information — for us to deanonymize location data.” The *Times* was able to track the movements of President Trump via a member of his Secret Service detail. Deanonymized data may be useful for commercial and/or intelligence purposes.

~~SECRET~~ / [REDACTED]

~~SECRET~~ // [REDACTED]

~~SECRET~~ // [REDACTED]

~~SECRET~~ / [REDACTED]

2. (U) THE ROLE OF CAI IN INTELLIGENCE COLLECTION AND ANALYSIS

(U//FOUO) CAI clearly provides intelligence value, whether considered in isolation and/or in combination with other information, and whether reviewed by humans and/or by machines. The IC currently acquires a significant amount of CAI for mission-related purposes, including in some cases social media data [REDACTED] and many other types of information. As a resource available to the general public, including adversaries, CAI also raises counter-intelligence risks for the IC. It also has increasingly important risks and implications for U.S. person privacy and civil liberties, as CAI can reveal sensitive and intimate information about individuals. Without proper controls, CAI can be misused to cause substantial harm, embarrassment, and inconvenience to U.S. persons. The widespread availability of CAI regarding the activities of large numbers of individuals is a relatively new, rapidly growing, and increasingly significant part of the information environment in which the IC must function. That is the core of why it was necessary and appropriate for the IC to recognize the complex issues inherent in modern CAI and to commission this report.

2.1. (U) CAI as a Source for OSINT. For the IC, CAI provides intelligence value as a form of publicly available information used to create Open Source Intelligence (OSINT), as well as for other purposes including force protection and enrichment of information in other INT disciplines. Many recent commissions and reports have focused on the value of CAI and other PAI as OSINT. For example, in 2005, the WMD Commission's [report](#) concluded (pages 22-23) that "analysts who use open source information can be more effective than those who don't," and urged creation of an "entity that collects, processes, and makes available to analysts the mass of open source information that is available in the world today." Similarly, the January 2019 "[AIM Initiative](#)" from the Office of the Director of National Intelligence (ODNI), which is a strategy for augmenting intelligence using machines, explained "the IC must develop both the capability and capacity to take advantage of available data across all INTs and open source, and develop AI solutions that process and relate information from multiple modalities." A January 2021 [report](#) from the Center for Strategic and International Studies (CSIS) notes that the IC must "encourage IC agencies to integrate OSINT into collection and analytic tradecraft," because the "combination of cloud, cloud-based AI and analytics tools, and commercial GEOINT and SIGINT collection means that high-quality, multi-source intelligence analysis can be produced at the unclassified level from anywhere equipped to do so."

2.2. (U) Examples of CAI Contracts. The IC currently acquires a large amount of CAI. Unclassified IC and other contracts for CAI can be found at [Sam.Gov](#), a U.S. government website that allows searching by agency or sub-agency and by keywords, among other things. By way of example only, this website shows that the following agencies have, have had, have considered, or are considering the following contracts or proposals related to CAI:

- (U) The Federal Bureau of Investigation (FBI) with [ZeroFox](#) for social media alerting ([15F06721P0002431](#))

~~SECRET~~ / [REDACTED]

~~SECRET~~ // [REDACTED]

- [REDACTED]
- (U) The Defense Intelligence Agency (DIA) for social media reports on individuals who are seeking a security clearance ([HHM402-16-SM-CHECKS](#)), and with LexisNexis for “retrieval of comprehensive on-line search results related to commercial due diligence from a maximum number of sources (news, company, public records, legal, regulatory financial, and industry information),” among other things ([HHM402-21-Q-0094](#))
- (U) The U.S. Navy with Sayari Analytics, Inc. for access to its database that “contains tens of thousands of previously-unidentified specific nodes, facilities and key people related to US sanctioned actors including ‘2+3’ threats to national security” ([N0001518PR11212](#))
- (U) Various offices within the Treasury Department for access to Banker’s Almanac ([RFQ-FIN-55100-21-0010](#))
- (U) The Department of Defense (DOD) for access to Jane’s online ([W31P4Q17T0009](#))
- (U) The Coast Guard with Babel Street for “Open Source Data Collection, Translation, Analysis Application” ([70Z08419QVA044](#)).

(U) In addition, DIA has provided the following information about a CAI contract in an unclassified and publicly-available [paper](#) sent to Congress on January 15, 2021:

(U) DIA currently provides funding to another agency that purchases commercially available geolocation metadata aggregated from smartphones. The data DIA receives is global in scope and is not identified as “U.S. location data” or “foreign location data” by the vendor at the time it is provisioned to DIA. DIA processes the location data as it arrives to identify U.S. location data points that it segregates in a separate database. DIA personnel can only query the U.S. location database when authorized through a specific process requiring approval from the Office of General Counsel (OGC), Office of Oversight and Compliance (OOC), and DIA senior leadership. Permission to query the U.S. device location data has been granted five times in the past two-and-a-half years for authorized purposes.

(U) In the process of preparing this report, DHS described for us three ways in which CAI is generally used by its Office of Intelligence and Analysis (I&A):

- (~~U//FOUO~~) Web of Science is a powerful targeting tool, as it allows DHS I&A analysts to quickly and efficiently search and triage a large repository of academic publications and filter according to funding sources, affiliations, co-authors, and other key terms. This

~~SECRET~~ // [REDACTED]

~~SECRET~~ / [REDACTED]

service provides critical insight into academic publications that are not easily found elsewhere or are hidden behind paywalls when searched via other means, such as Google Scholar. For example, using Web of Science, DHS I&A analysts have identified foreign researchers studying in the United States with previously unknown associations with their home country's military. Additionally, through the currently OSDLS-managed subscriptions, we are also able to access the Web of Science API, which allows us to apply data analytics to the database.

- (U//~~FOUO~~) CLEAR enables DHS I&A to resolve identities and also provides leads for further analysis in DHS systems, thereby focusing resources on threat actors and not innocent persons. Commercial databases like CLEAR often have current location and contact information as well. Often, given the target set we focus on – non-traditional collectors – intelligence collection is not sufficient to resolve identities of subjects of interest. Data available in a commercially available datasets enables identity resolution by comparing it to what's in DHS systems and also reduces the risk of misidentification.
- (U//~~FOUO~~) Dun and Bradstreet and similar tools enable DHS I&A to resolve private companies' primary enterprises with their subsidiaries/affiliates and provides leads for further analysis in DHS systems and classified databases. Access to this information is critical to countering malign foreign investment that may threaten the security and resiliency of U.S. critical infrastructure.

2.3. (U) Examples of CAI Value. In our classified briefings with IC elements, we discussed the intelligence value of CAI, including how it can be used to reduce cost and risk of acquisition that might otherwise occur through clandestine means. The IC is strongly of the view that it will be at a significant disadvantage vis a vis foreign adversaries and competitors if it does not enjoy certain access to CAI. We urge the IC to make available several unclassified examples showing the value of CAI because we believe it will help inform the policy debate, in keeping with [Principles of Intelligence Transparency for the IC](#). The IC has done this in the past in other contexts, including for [Section 702 of the FISA Amendments Act](#).

(U) Here are two unclassified examples provided by the IC in response to our request while we were preparing this report:

- (U//~~FOUO~~) "NSA's Cybersecurity Collaboration Center leveraged commercial and SIGINT sources to expand the community sight picture on the advanced persistent threat Cobalt Strike actor. Analysts used enterprise access from [REDACTED] and others to identify a pattern in the registration of the seed nodes shared by the 370 domains – of which 19 were tagged by [REDACTED] and of those, 7 resolved to CobaltStrike infrastructure. A pattern in uniform resource locators (URLs) was also discovered to be associated with CobaltStrike using CAI which led to the discovery of an additional 49 internet protocol (IP) addresses."

~~SECRET~~ / [REDACTED]

~~SECRET~~ // [REDACTED]

- (U//~~FOUO~~) “CAI allows the IC to create valuable products for excluded missions like HADR [humanitarian assistance and disaster response]. These products are similar to those created by the commercial and academic community. These types of use cases focus on providing strategic level analytic outputs on how events affect human mobility at-scale or the country level. Examples include but are not limited to, how natural disasters and the spread of disease affect the movement of humans and vice versa.”

(U) We expect that the IC will be able to provide additional unclassified examples over time. If necessary, moreover, classified examples should be made available to appropriate audiences. We believe that CAI is extremely and increasingly valuable and important for the conduct of modern intelligence activity, both as a source of OSINT and to support, enrich and enable other INT disciplines.

2.4. (U) Non-Analytic Uses of CAI. It is important to recognize that in some cases, CAI may also be used for purposes other than intelligence collection and analysis. At the outset, of course, the FBI uses CAI under its law enforcement authorities, as authorized in AG Guidelines and FBI policy, for the investigation of criminal matters, and non-intelligence elements of DOD may also use CAI for their missions. We also briefly consider three non-analytic intelligence use cases of CAI.

(U//~~FOUO~~) First, CAI may be useful in supporting compliance with legal or policy requirements. For example, geolocation CAI might be able to support compliance with 50 U.S.C. § 1881a (Section 702 of the FISA Amendments Act), which generally applies only to collection targeting non-U.S. persons reasonably believed to be located outside the United States. CAI can help determine location for compliance with this core requirement of Section 1881a. It may also be useful in complying with requirements established by Congress for situations in which non-U.S. persons abroad who are under surveillance travel into the United States. See 50 U.S.C. § 1805(f). More generally, CAI may also help establish the “foreignness” of SIGINT or other collection targets as necessary to meet legal or policy requirements.

(U//~~FOUO~~) Second, CAI may also be used in support of clandestine and HUMINT operations. CAI utilized in support of operations uniquely enables activities like cover development and operations planning. These activities are tightly held within the IC and subject to extremely restrictive operations access and handling rules. Further, CAI data obtained to support operations is outside the IC’s classic analysis and intelligence reporting streams – it is not disseminated.

(U) Third, CAI may be useful in building and training artificial intelligence models. Although non-analytical in the strict sense, such models themselves can then be used to gain analytic insight or for other purposes.

~~SECRET~~ // [REDACTED]

~~SECRET~~ / [REDACTED]

(U) We do not mean to suggest a policy outcome in these particular use cases. Our only point is that policy questions concerning CAI are not one-dimensional. The importance and nature of the need, the absence of viable alternatives for meeting it, restrictions on access to and use and dissemination of data, should all be considered in reaching an appropriate policy judgment in each case – assuming, as always, that outcomes are not dictated by law. It may be, for example, that certain privacy-protecting methods, such as encrypting, masking, and use of differential privacy, may be viable for some mission needs even if not for others.

2.5. (U) Counter-Intelligence Risks in CAI. There is also a growing recognition that CAI, as a generally available resource, offers intelligence benefits to our adversaries, some of which may create counter-intelligence risk for the IC. For example, the January 2021 CSIS report cited above also urges the IC to “test and demonstrate the utility of OSINT and AI in analysis on critical threats, such as the adversary use of AI-enabled capabilities in disinformation and influence operations.” Additional risks are developed in this April 2021 Lawfare [article](#) and this August 2021 [report](#) from Duke University.

(U) The Duke University report describes certain counter-intelligence risks from CAI. It finds, for example, that of 10 major data brokers surveyed, three advertise that they can provide data to identify U.S. military personnel. The report goes on to note (as summarized in a Lawfare [article](#) by its author): “Foreign actors could use this data to bolster their influence campaigns to interfere in U.S. electoral processes. Criminal organizations could use this data to build profiles on and subsequently target prosecutors and judges. Foreign intelligence organizations could acquire this data through a variety of means—including through front companies that could legally purchase the data from U.S. brokers and through simply hacking a data broker and stealing it all—to build profiles on politicians, media figures, diplomats, civil servants, and even suspected or secretly identified intelligence operatives.”

(U) We have not necessarily validated these examples with the IC, meaning that they should not necessarily be taken as unresolved risks; but they illustrate the types of risk that CAI can create in the hands of our adversaries.

2.6. (U) Sensitivity of CAI. CAI can reveal sensitive and intimate information about the personal attributes, private behavior, social connections, and speech of U.S. persons and non-U.S. persons. It can be misused to pry into private lives, ruin reputations, and cause emotional distress and threaten the safety of individuals. Even subject to appropriate controls, CAI can increase the power of the government’s ability to peer into private lives to levels that may exceed our constitutional traditions or other social expectations. Mission creep can subject CAI collected for one purpose to other purposes that might raise risks beyond those originally calculated. The IC’s use of CAI is also the subject of intense scrutiny and speculation by political leaders, the news media, and civil society.

~~SECRET~~ / [REDACTED]

—SECRET// [REDACTED]

2.6.1. (U) CAI Includes Sensitive and Intimate Information. CAI can contain information that is deemed sensitive, meaning information that is not widely known about an individual that could be used to cause harm to the person's reputation, emotional well-being, or physical safety. As a primary justification for finding precise cell-site location information subject to Fourth Amendment protection in Carpenter v. United States, 138 S. Ct. 2206 (2018), the Supreme Court focused on how the "data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.' These location records 'hold for many Americans the 'privacies of life.'" *Id.* at 2217. CAI can also contain intimate information, meaning information that reveals private details about how people relate to one another.

2.6.2. (U) Defining Sensitivity Categorically. Many statutes, rules, and privacy policies describe information sensitivity categorically, listing types of information that tend to raise risks of harm. To give a comparative example, the European General Data Protection Regulation (GDPR) identifies as sensitive:

(U) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership., and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

(U) Similarly, an internal data call from ODNI listed several categories of CAI as potentially sensitive, including:

(U) persistent location information, medical (to include mental health) information, travel records, attorney-client information, information concerning ... religion or religious practices, information containing data on sexual activity, records regarding purchases, library records [as well as information] regarding individuals' communications [metadata and content] [and] information concerning individuals' expression of ideas or political views or the groups or individuals with whom they associate.

2.6.3. (~~U//FOUO~~) CAI Can Be Misused. Studies document the extent to which large collections of sensitive and intimate information about individuals, CAI or not, can be subject to abuse. Documented examples of LOVEINT abuses (government officials spying on actual or potential romantic partners) involving other intelligence collections demonstrate the potential for comparable abuse of CAI held by the IC. In the wrong hands, sensitive insights gained through CAI could facilitate blackmail, stalking, harassment, and public shaming. Concerns like these are why, as detailed in Part 4, several IC elements require a "volume, proportion, and sensitivity" analysis of certain data practices that considers, among other things, the "potential for substantial harm, embarrassment, inconvenience, or unfairness to U.S. persons if the information is improperly used or disclosed."

—SECRET// [REDACTED]

~~SECRET~~ / [REDACTED]

2.6.4. (U) CAI Increases the Power of the Government. The government would never have been permitted to compel billions of people to carry location tracking devices on their persons at all times, to log and track most of their social interactions, or to keep flawless records of all their reading habits. Yet smartphones, connected cars, web tracking technologies, the Internet of Things, and other innovations have had this effect without government participation. While the IC cannot willingly blind itself to this information, it must appreciate how unfettered access to CAI increases its power in ways that may exceed our constitutional traditions or other societal expectations.

(U) CAI also implicates civil liberties. CAI can disclose, for example, the detailed movements and associations of individuals and groups, revealing political, religious, travel, and speech activities. CAI could be used, for example, to identify every person who attended a protest or rally based on their smartphone location or ad-tracking records. Civil liberties concerns such as these are examples of how large quantities of nominally “public” information can result in sensitive aggregations.

2.6.5. (U) Aggregation of CAI Raise the Risk of Mission Creep. CAI collected for one purpose may be reused for other purposes. An assessment of the risk to privacy of data collected at one point in time may differ materially from a reassessment of the risk as applied to new purposes.

2.6.6. (U) Public, Media, and Political Scrutiny. The public seems to care about the risk to personal privacy posed by the accumulation and sale of personal information by online platforms, smartphone apps, connected devices, and other commercial entities. A steady string of public controversies including Cambridge Analytica, the revelations by the *New York Times* about data brokers that sell location information, the use of app usage data to identify a priest who was using the Grindr app, and the revelation of the sale of usage data by a Muslim prayer app, among many other examples, demonstrate the keen interest in CAI, at least on the part of the media, civil society groups, and political leaders. The possible future revelation that any component of the IC has gathered CAI without a proper accounting for the costs and benefits raises the risk of significant media attention and political fallout and could jeopardize other forms of CAI collection and use.

2.6.7. (U) Need for Thoughtful Approach. None of this is to suggest that CAI should be categorically off-limits to the IC; the CAI that we address is publicly available, including to friendly and adversarial foreign governments (and their intelligence services), non-governmental organizations, commercial entities of many kinds, and individuals. It is only to say that the privacy and civil liberties concerns that underlie judicial decisions like *Carpenter*, and possible legislation restricting access to CAI, are real and important, and that the IC should therefore take responsibility to develop a thoughtful and balanced approach in this area.

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

(U) As noted above, we think it is insufficient as a matter of policy to treat all CAI as PAI, without more, because modern CAI is so different from traditional PAI. Today's CAI is more revealing, available on more people (in bulk), less possible to avoid, and less well understood than traditional PAI. It is only a little oversimplified to say that when Executive Order 12333 was adopted, U.S. persons generally understood that the White Pages and the *New York Times* were public, but also understood that it was possible to choose an unpublished telephone number and (usually) to keep oneself out of the newspaper. Today, in a way that far fewer Americans seem to understand, and even fewer of them can avoid, CAI includes information on nearly everyone that is of a type and level of sensitivity that historically could have been obtained, if at all, only through targeted (and predicated) collection. As a matter of policy, therefore, asserting that modern CAI is materially indistinguishable from traditional PAI "is like saying a ride on horseback is materially indistinguishable from a flight to the moon." [Riley v. California](#), 573 U.S. 373, 393 (2014). These new qualitative and quantitative aspects of CAI, particularly of or concerning U.S. persons and as discussed in Section 4.3.4, are key sensitivity concerns that animate the need for a new approach.

2.7. (U) Summary. We have no doubt that CAI can provide significant intelligence value, both to the IC and to our adversaries, whether standing alone or in combination with other information that is collected using classified sources and methods, and whether analyzed by humans and/or by machines. It also clearly raises significant issues of privacy and sensitivity, including for U.S. persons. CAI is a relatively new, rapidly growing, and increasingly significant part of the information environment in which the IC must function. That is the core of why this report is necessary.

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

3. (U) THE EXISTING POLICY FRAMEWORK FOR CAI

(U) *Under the U.S. Constitution, federal statutes, and IC elements' internal procedures, CAI is generally less strictly regulated than other forms of information acquired by the IC, principally because it is publicly available. In our view, however, changes in CAI have considerably undermined the historical policy rationale for treating PAI categorically as non-sensitive information, that the IC can use without significantly affecting the privacy and civil liberties of U.S. persons. For example, under [Carpenter v. United States](#), acquisition of persistent location information (and perhaps other detailed information) concerning one person by law enforcement from communications providers is a Fourth Amendment "search" that generally requires probable cause. However, the same type of information on millions of Americans is openly for sale to the general public. As such, IC policies treat the information as PAI and IC elements can purchase it. While IC policies regulate such information based on the volume, proportion and sensitivity of USPI it contains, those policies may not accord sufficient protection to information that is now broadly understood to be sensitive. It is not sufficient as a matter of policy simply to say that CAI is PAI; and saying so without more may be affirmatively confusing to intelligence professionals.*

3.1. (U) PAI. Historically, PAI has not been considered sensitive, as reflected in both U.S. law and policy. In keeping with our TOR, we do not offer an independent legal analysis of this issue; instead, we review the legal background governing PAI solely as context for our policy discussion of CAI.

3.1.1. (U) Constitutional Provisions. As a general matter, under the Fourth Amendment, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." [Katz v. United States](#), 389 U.S. 347, 351 (1967). To be sure, more recent decisions, most notably [Carpenter v. United States](#), 138 S. Ct. 2206 (2018), raise questions about the extent to which providing information to certain third parties can extinguish a reasonable expectation of privacy in that information. In keeping with our TOR, we do not attempt to answer those questions; it is enough for our purposes to recognize the general rule that PAI is not deemed sensitive. To take an obvious example, the Justices' signed opinions in *Carpenter* are clearly not protected by the Fourth Amendment and are available in searchable CAI data sets from Lexis, Westlaw, and other providers. Historically, PAI also generally was not considered sensitive under the First Amendment; but PAI today, including CAI, may implicate First Amendment rights.

3.1.2. (U) Federal Statutes. Resting on the constitutional understanding discussed above, many federal statutes expressly decline to protect, and assume the absence of Fourth Amendment protection for, PAI. The federal Wiretap Act, 18 U.S.C. § 2511(2)(g)(i), provides that it "shall not be unlawful . . . for any person . . . to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." Similarly, the Foreign Intelligence

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

Surveillance Act defines “electronic surveillance” in ways that expressly incorporate Fourth Amendment principles and law enforcement standards, 50 U.S.C. §§ 1801(f), and requires “minimization” of “nonpublicly available information,” 50 U.S.C. § 1801(h). To be sure, the Privacy Act, 5 U.S.C. § 552a, also places certain restrictions on the IC when it collects and retrieves USPI, including when the USPI is also PAI. The IC must have clear authority and mission need to collect this PAI; must provide a notice to the public about the collection (system of records notices), and generally may not maintain a record describing how an individual exercises First Amendment rights. Some PAI can include protected speech (e.g., social media posts) or associational information, and the Privacy Act would need to be considered before collecting such information.

3.1.3. (U) Pending Legislation. We are aware that there are federal legislative efforts underway that might affect the treatment of CAI, at least as acquired by the IC or other governmental entities. We do not express an opinion on the merits of any particular pending or contemplated legislation, but as an institutional matter we believe that legislation could address policy concerns with the current regulatory framework governing CAI.

3.1.4. (U) IC Policy. The foundational document governing the IC also treats PAI as relatively unprotected. Section 2.3 of [Executive Order 12333](#) authorizes IC elements “to collect, retain, or dissemination information about U.S. persons” in accordance with procedures established by the head of the IC element and the Attorney General, and provides that these procedures “shall permit collection, retention, and dissemination of . . . [i]nformation that is publicly available or collected with the consent of the person concerned.” The term “publicly available” is defined in the procedures of several IC elements. For example, the procedures for the Central Intelligence Agency (CIA) define “publicly available information” is as follows:

(U) [1] information that has been published or broadcast for public consumption, [2] is available on request to the public, [3] is accessible online or otherwise to the public, [4] **is available to the public by subscription or purchase**, [5] could be seen or heard by any casual observer (but not amounting to physical surveillance), [6] is made available at a meeting open to the public, or [7] is obtained by visiting any place or attending any event that is open to the public.

(U) Information is publicly available only if it is made available to the CIA under conditions or on terms generally applicable to the public. For example, certain commercially acquired data may be considered publicly available if a non-U.S. government person or corporation could acquire that same data in that same way from that same commercial source; however, other commercial acquisitions of data may be so tailored and specialized for government use, and unavailable to a similarly situated private-sector purchaser, that the data cannot be considered publicly available.

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

(U) CIA [Guidelines](#) § 12.20 (emphasis added). The corresponding guidance for DOD intelligence elements adopts a similar definition and adds the clarification that “Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public.” DOD [Manual](#) 5240.01 §§ 3.2.b and G-2 at page 53.

(U) Under Executive Order 12333, moreover, some IC elements are authorized to collect information (mainly or exclusively) “overtly or through publicly available sources.” EO 12333 §§ 1.7(i)-(j), 1.8, 1.9, 1.12(c). The expansion of PAI to include modern CAI is highly consequential for the work of these IC elements.

3.1.5. (U) [IC Guidance](#). In July 2011, ODNI issued [Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publicly Available Information](#). This guidance included a “shorthand, non-exhaustive list of factors to consider for properly obtaining and using” PAI, including that the PAI is (1) available to the general public; (2) lawfully obtained by the IC (e.g., if a hacker posts instructions on a blog for how to penetrate a bank’s online security, the bank’s data does not become lawfully available as a result); (3) the IC purchaser has complied with any requirements to disclose IC affiliation, which is often addressed through guidelines on “undisclosed participation” and similar rules; (4) requirements for U.S. person information, including as to purpose, retention, and dissemination, are met; and (5) there are safeguards in place to ensure that the information is used in a manner that satisfies IC standards for “information accuracy, quality, and reliability,” including those in [ICD 203](#). Although this guidance is more than a decade old, we believe that it is valuable and could be updated as discussed further below.

3.2. (U) [CAI](#). As discussed above, the definition of PAI in modern IC guidelines includes CAI to the extent that it “is available to the public by subscription or purchase.” That description applies to much CAI, and as previously noted it is the focus of our report, to the exclusion of CAI products that are available only to governments. As noted above, IC elements’ guidelines recognize that while some CAI is PAI, other commercial acquisitions of data may be so tailored and specialized for government use, and unavailable to a similarly situated private-sector purchaser, that the data cannot be considered publicly available. Approaching the issue from the other side, there are certain legal restrictions on providing CAI to the U.S. government as opposed to other purchasers (see, e.g., 18 U.S.C. § 2702(a)(3)), as well as potential limits on those restrictions (see, e.g., 18 U.S.C. § 2511(2)(F)). In substantial part, however, CAI is available to the IC much as it is to the general public, other private-sector entities and non-governmental organizations (NGOs), and foreign governments.

3.3. (U) [CAI Under IC Guidelines](#). As we understand it, here is the process, in the form of issues and questions, that the CIA and DOD Attorney General guidelines (issued under Section 2.3 of Executive Order 12333) prescribe for potential acquisition and treatment of CAI (other IC

~~SECRET~~ / [REDACTED]

~~SECRET~~ // [REDACTED]

elements have their own guidelines, some of which at this writing are in the process of being revised).

3.3.1. (U) Authorized Purpose. This is required for all activity under the IC guidelines. For example, as a general matter, the CIA may collect information, including information concerning U.S. persons and U.S. Person Identifying Information (USPI or USPII, depending on the agency), only if the collection has “a purpose consistent with [lawful] CIA authorities and responsibilities.” CIA Guidelines § 3.3. Similarly, as a general matter the DOD Manual permits intentional acquisition of USPI “only if the information sought is reasonably believed to be necessary for the performance of an authorized intelligence mission or function assigned to the [DOD] Component” conducting the acquisition. DOD Manual § 3.2.c; see *id.* § 3.2.f(2). These baseline requirements preclude, for example, intelligence collection for domestic political purposes. See, e.g., CIA Guidelines § 3.3 (“CIA is not authorized to and shall not collect or maintain information concerning U.S. persons solely for the purpose of monitoring (1) activities protected by the First Amendment or (2) the lawful exercise of other rights secured by the Constitution or laws of the United States ... CIA is not authorized to and shall not engage in any intelligence activity, including dissemination of information to the Executive Office of the President, for the purpose of affecting the political process in the United States”); see also [The Attorney General’s Guidelines for Domestic FBI Operations](#). These limitations are themselves derived from and consistent with Sections 2.3 and 2.4 of Executive Order 12333 and other provisions of law.

3.3.2. (U) Publicly Available. Where the IC has an authorized intelligence purpose, and the information it seeks is reasonably believed to be necessary for that purpose, it generally may collect information, including USPI, if the information is publicly available. See, e.g., DOD Manual § 3.2.c.(1); CIA Guidelines §§ 4.2(a), 4.21.

3.3.3. (U) Scope of Collection. The CIA’s guidelines permit the use of a collection technique “only if a less intrusive technique cannot acquire intelligence of the nature, reliability, and timeliness required,” and they treat collection of publicly available CIA as a “basic” collection technique, generally the least intrusive category. CIA Guidelines §§ 4.1-4.2. However, the CIA Guidelines also require (§ 3.3) that in “any collection activity, the CIA shall collect only the amount of information reasonably necessary to support [an authorized] purpose.” Where a collection exceeds the agency’s ability promptly to evaluate all of the collected information for retention, the CIA guidelines require the approving official to document “the collection technique(s) employed, including any reasonable steps that were or will be taken to limit the information to the smallest separable subset of data containing the information necessary to achieve the purpose of the collection,” such as the use of “filters or similar technology” that “should be applied as early as practicable in the course of the collection activity.” *Id.* § 5.2(c). The CIA Guidelines explicitly address and require additional documentation for bulk collection (information collected without discriminants). See *id.* §§ 5, 12.2. The DOD Manual provides that in addition to using the “least intrusive means” of collection, § 3.2.(f)(3)(a), “in collecting non-

~~SECRET~~ // [REDACTED]

~~SECRET~~ / [REDACTED]

publicly available USPI,” DOD components “will, to the extent practicable, collect no more information than is reasonably necessary.” DOD Manual § 3.2.f.(3)(a), 3.2.f.(4). By its terms, this last requirement does not apply to PAI, although DOD’s rules on the volume, proportionality, and sensitivity (VPS) of USPI, discussed immediately below, do apply if the CAI includes USPI. Current understandings of CAI as a subset of PAI mean that IC elements are essentially encouraged to acquire CAI, when it is PAI, over other sources of information.

3.3.3.1. (U) Clarification of Current Guidelines. The IC may want to recalibrate, clarify or consider its understanding of whether and how the preference for collection using the “least intrusive means” relates to a preference to collect information that is necessary for an authorized purpose. The increasing availability of CAI means that potentially sensitive information on large numbers of persons may be PAI. In some cases, therefore, collecting a large dataset using commercial means might invade privacy more than a narrower collection using means that target a specific individual or smaller group. New guidance from some IC elements addresses some of these issues (see, e.g., discussion of DIA procedures below).

3.3.4. (U) Volume, Proportion, Sensitivity (VPS) of USPI. The DOD Manual defines a category known as “Special Circumstances Collection” according to the “volume, proportion, and sensitivity of USPI likely to be acquired, and the intrusiveness of the methods used to collect the information,” including when the information is PAI. DOD Manual § 3.2.e. When “special circumstances exist, the DOD component head or delegate must determine whether to authorize the collection and, if so, whether enhanced safeguards are appropriate.” *Id.* The CIA Guidelines address “volume proportion, and sensitivity” of USPII in “exceptional handling requirements” that apply to unevaluated data sets and might require “additional access approvals or additional training requirements,” among other things. CIA Guidelines § 6.2. Some IC elements have established, or are in the process of developing, more detailed VPS guidance, as discussed in Part 4.

3.4. (U) CAI & Carpenter. Although to our knowledge the IC has not arrived at a community-wide formal position on the issue, at least one IC element, the Defense Intelligence Agency (DIA), has advised Congress in [writing](#) that, as of January 15, 2021, it “does not construe the *Carpenter* decision to require a judicial warrant endorsing purchase or use of commercially-available data for intelligence purposes.” We do not express a view on the legal merits of this position, in keeping with our TOR, but in an effort to provide context for readers of this report, we believe that it may rest on one or more of the following theories: (1) certain forms of CAI do not implicate the privacy or Fourth Amendment rights of any data subject (e.g., topographical maps); (2) some CAI involves data and other factors that bring the acquisition outside the scope of *Carpenter*, meaning that normal third-party doctrine (e.g., [United States v. Miller](#), 425 U.S. 435 (1976)) extinguishes any rights in the data subject; (3) for data types and acquisition modes that are subject to *Carpenter*, the decision does not apply to the “special need” of intelligence collection conducted by the IC; (4) even if *Carpenter* does apply, it would at most create a shared Fourth Amendment interest among the data seller and the data subject, meaning that

~~SECRET~~ / [REDACTED]

~~SECRET~~ // [REDACTED]

the seller may consent unilaterally to sell the CAI, at least where the subject is not present and objecting to the sale (e.g., [United States v. Matlock](#), 415 U.S. 164 (1974); [Fernandez v. California](#), 571 U.S. 292 (2014) – a consent-based Fourth Amendment doctrine that is orthogonal to and unchanged by *Carpenter*).

(~~U//FOUO~~) At the same time, however, ODNI has [taken the position in writing](#) that, while *Carpenter*'s reach remains uncertain, the IC will collect persistent location data under FISA's provisions requiring probable cause and applicable to collection of communications "contents" rather than metadata, which is a clear effort to hedge against the possible application of *Carpenter* to foreign intelligence collection. This is not meant to suggest internal legal disagreement within the IC, but only to say that IC elements can and have made policy judgments designed to hedge against the possibility that *Carpenter* applies beyond its facts, or otherwise to address the concerns that underlie it.

~~SECRET~~ // [REDACTED]

~~SECRET~~ // [REDACTED]

4. (U) RECOMMENDATIONS

~~(U//FOUO)~~ We have three recommendations. **First**, the IC should develop a multi-layered process to catalog, to the extent feasible, the CAI that IC elements acquire. This will be a complex undertaking requiring attention to procurement contracts, functionally equivalent data acquisition processes, data flows, and data use. The IC cannot understand and improve how it deals with CAI unless and until it knows what it is doing with CAI. **Second**, based on that knowledge, the IC should develop a set of adaptable standards and procedures for CAI, governing and requiring regular re-evaluation of acquisition and other decisions. **Third**, as part of this set of standards and procedures, and/or as a complement to it, the IC should develop more precise sensitivity and privacy-protecting guidance for CAI. PAI is no longer a good proxy for non-sensitive information; today, much CAI is very sensitive, and the IC therefore needs to develop more refined approaches.

4.1. ~~(U//FOUO)~~ Recommendation #1: The IC Should Learn How It Acquires and Uses CAI. As discussed in Part 1, changes in digital technology and related factors have created a large and growing market for CAI that includes significant VPS of USPI but remains PAI under current IC guidelines. CAI is very valuable as a source of intelligence insight and creates significant risks to privacy. But the IC does not currently have sufficient visibility into its own acquisition and use of CAI across its 18 elements. Accordingly, our first recommendation is for the IC to implement a process that affords it better insight, on a going-forward basis, as to that acquisition and use.

4.1.1. ~~(U//FOUO)~~ The Value of Understanding. Given the increasing importance of CAI, and the highly dynamic nature of available offerings and markets, the IC is rightly focused on understanding its own collection and use of CAI. Insight gained from 18 IC elements could inform community-wide best practices in several areas, including means and terms of acquisition, analysis and other approaches to use and exploitation (e.g., increased awareness of the intelligence value of CAI to the IC and to our adversaries), awareness of privacy and other sensitivities, and applicable legal and policy rules and frameworks. Cf. [ICD 501](#). Logically inconsistent approaches to CAI (as opposed to mere differences in approach, which properly may result from differences in mission, authorities, and other factors) can be found and addressed. In addition, overseers will rightly pose questions about the IC's approach to CAI, and the IC should be able to answer those questions with high fidelity and confidence.

4.1.2. (U) Prospective Cataloguing Effort. For three main reasons, we recommend that the IC pursue a forward-looking and recurring effort to understanding its own use of CAI. As part of that process, of course, the IC will need to navigate security and counterintelligence concerns.

(U) First, prior retrospective data calls have not fully succeeded. An attempt from the beginning of 2021 did not return comprehensive and reliable results, and – in part for that reason – the data call underlying our report sought only representative samples of CAI. That data call has served us well, and when combined with insights from our discussions with IC elements we

~~SECRET~~ // [REDACTED]

~~SECRET~~ / [REDACTED]

believe it provides a suitable foundation for our report and recommendations. Our report is not, however, based on anything approaching a complete survey of the use of CAI by the IC, and difficulties in accessing historical information about the use of CAI informs our recommendation for a new, forward-looking approach. Depending on what is revealed by that forward-looking approach, significant new work may be required. For example, as noted throughout this report, our report addresses CAI that is publicly available; if it turns out to be the case that the IC acquires and uses a significant amount of CAI that is not PAI (e.g., because it is sold only to governmental customers, not to the general public), then further analysis on that issue probably would be necessary.

(U) Second, we believe that a prospective effort will be valuable. The IC's acquisition and use of CAI, as well as the overall market for CAI, is very dynamic, making a retrospective survey less informative and useful for developing new approaches.

(U) Third, and relatedly, a forward-looking process that recurs could capture both current and future states of affairs concerning CAI, allowing the IC to keep up with what we expect will be significant developments over time.

4.1.3. (U) Multi-Layered Cataloguing Effort. We recommend that the IC's forward-looking process for cataloguing CAI be multi-layered.

(U) At the outset, the cataloguing effort should include formal contracts and procurement decisions, as well as functionally equivalent agency-specific data acquisition processes, because these will help identify CAI when it first arrives at (or becomes available to) an IC element. By "functionally equivalent agency-specific data acquisition processes," we mean to cover acquisition of CAI that occurs without a formal procurement decision, such as when CAI is provided (for ingestion or via a licensed right of access) to an IC element from a non-IC element, including U.S. Title 10 elements, law enforcement, foreign governments, and non-governmental organizations. These processes may vary from one IC element to another and over time within an IC element. Even within an explicit procurement setting, the role of CAI may not always be apparent – e.g., when a contract is for services, rather than for provisioning of CAI *per se*, but the services in question require the use of CAI by the service-provider.

(U) Given these complexities in the acquisition of CAI, we also recommend that the IC focus detection efforts at later stages of the information lifecycle, including in the process of planning for and actually using data. We assess that this multi-layered approach is the best way efficiently to begin capturing CAI acquisitions and use, including CAI acquired in bulk (or otherwise in substantial amounts).

(U) In particular, key inputs to the cataloguing process may include (1) documentation reflecting the purchase, license, or other acquisition of a CAI dataset; (2) audits by chief information officers (CIOs) and chief data officers (CDOs) responsible for monitoring data flows

~~SECRET~~ / [REDACTED]

~~SECRET~~ // [REDACTED]

across agency systems and repositories; and (3) sourcing, citation and survey data from collection officers and intelligence analysts reflecting the exploitation of specific CAI sources to support tipping, queuing, finished intelligence (FINTEL), and other intelligence products.

(U) If the IC finds that it acquires CAI through mechanisms outside the scope of what we have described in this report, then of course those mechanisms should be examined as well. Here, as in the definition of CAI, attempts to describe a formal scope of effort should not obscure the functional focus on gaining the best possible understanding of the CAI that is actually being acquired and used by the IC.

4.1.4. (U) Common Taxonomy and Understanding. A central goal of the forward-looking process should be to develop an IC-wide common taxonomy and understanding of CAI, to permit meaningful comparisons and analysis at the scale of current and anticipated future CAI operations. Of course, different IC elements will naturally and rightly adopt different standards and procedures for CAI, according to their missions, authorities, need for CAI (and the sensitivity and other attributes of the CAI they need), and other factors. But our assessment is that current practices vary more, and more unsystematically, than is best. Put differently, the IC's approach to CAI so far has been mainly federated, with individual elements operating as what might be called laboratories of CAI governance. Cf. [*New State Ice Co. v. Liebmann*](#), 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting). We think it is now time for the IC to assemble and identify best practices from the range of current practice, addressing both operational and risk/sensitivity frameworks, as discussed in our second and third recommendations, below.

4.2. (U) Recommendation #2: The IC Should Develop a Set of Adaptable Standards and Procedures for CAI. The IC should adopt an end-to-end approach for CAI. The IC does not currently have, and in our view should develop, a set of adaptable standards and procedures for CAI that can be applied across the community. This can be done centrally, for the IC or the Defense Intelligence Enterprise (DIE) as a whole, and/or at individual IC elements (where the approaches could vary from one element to another as long as they are consistent in principle). Either way, as the IC develops approaches to CAI, it will need to keep in mind IC elements' authorities and needs, and the ways in which they approach related issues. There is a well-understood tension, and need to balance, between consistency of approach across IC elements for any single data type, and consistency of approach within an IC element for related data types. We discuss immediately below the main issues of substance, structure, and process that we recommend be included in CAI standards and procedures, and then review and assess examples of such standards and procedures that are currently in effect at certain IC elements. Our third recommendation, discussed further below, addresses the need for enhanced sensitivity guidance for CAI, which overlaps in part with the issues discussed here.

4.2.1. (U) Issues. The IC should develop standards and procedures for CAI that address, among other things, the following issues:

~~SECRET~~ // [REDACTED]

~~SECRET~~ // [REDACTED]

- (U) Mission Analysis to Identify Need/Value. What problem is the acquisition of CAI designed to solve? How important is the problem, and how difficult is it to solve?
- (U) Fit Between Mission and CAI Data Set, Proposed Use. How will the CAI data set solve or address the problem? What other possible approaches are there for addressing the problem or meeting the need?
- (U) Vendor and Data Quality. This includes vendor capacity and longevity as well as quality/reliability issues pertaining to the vendor and its data sources and personnel. These factors may be more applicable to domestic commercial information acquisitions than foreign acquisitions. Can the vendor reliably meet the IC element's needs over time? What assurances of quality are available? Can the vendor adapt if circumstances or needs change?
- (U) Acquisition Mechanics. This includes where, how, and when CAI will be acquired; whether it will be ingested or accessed at the vendor; whether acquisition is overt or covert; whether USPI and other US data will be excluded at the vendor, at initial ingest by the IC element, in query returns, and/or not at all. It also includes ways in which acquisition mechanics may affect the IC's ability to use the data towards the mission need, including through the end user interface and application programming interfaces (APIs) if applicable. The USA Freedom Act illustrates the importance of the policy and engineering issues raised by acquisition mechanics.
- (U) Data Security. This involves potential counter-intelligence risk in the vendor and/or the method of acquisition, and in data storage within the IC element (it overlaps to some degree with the vendor and data quality review described above).
- (U) Sensitivity and Legal Review. This is focused on privacy protection and VPS of USPI and addressed further in Recommendation #3 below.
- (U) Auditing Use of CAI. This involves keeping copies of queries and similar uses of the CAI, and also finding ways to measure actual use and value over time.
- (U) Periodic Re-Evaluation. Finally, there should be a process to reconsider CAI acquisition and other decisions, to avoid inertial automatic renewal of contracts, and to take note when CAI data sources, or the use of CAI within the IC, change materially over time. Cf. ICD 203 and ICD 206, and more general principles of information integrity supporting standards of analytic tradecraft. In Recommendation #3, discussed below, we address re-evaluation to address VPS and sensitivity issues, a similar process with a different purpose than the re-evaluation discussed here.

~~SECRET~~ // [REDACTED]

~~SECRET~~ / [REDACTED]

- (U) Other Structural and Procedural Issues. Some IC elements have a dedicated unit or sub-unit focused on acquisition of CAI. Others have committees or working groups drawn from personnel in relevant sub-units. Both approaches are potentially viable, but IC elements should develop a regular process for addressing all of the issues listed above in regular order and with the benefit of relevant personnel. Results of decisions should be documented and provided to a central authority and assessed together periodically to discern best practices.

4.2.2. (U) Examples of Current CAI Approaches. Several IC elements have established standards and procedures to guide decisions on the acquisition and use of CAI. We review below the approaches taken by three agencies (relevant source materials are in the appendices). Some IC elements also have electronic Data Handling Forms (or the equivalent) governing acquisition of CAI that helpfully standardize aspects of the process for making CAI procurement decisions (or their functional equivalent).

4.2.2.1. (U) Treasury. The Treasury Department has chartered the Office of Terrorism and Financial Intelligence Data Governance Board. We have three main observations on the charter. First, the statement of objective and scope in Part B of the charter, and the statement of the Board's responsibilities in Part C, are general but broad enough to embrace the acquisition and handling of CAI, and it is our understanding that they are applied to CAI. But they do not explicitly apply to such acquisition and handling, and as Treasury advised, the Board was not created to address CAI *per se*, but rather to facilitate data integration and information sharing among all TFI components (one of which, OIA, is a member of the IC).

(U//~~FOUO~~) Second, while the Board allows for subject-matter experts to participate at the Chair's discretion under Part D.8 of the charter, the Board's regular members do not include representatives from privacy/civil liberties, which means that it may not be well positioned to address issues including VPS. We understand that privacy experts are, at least in some cases, invited to the Board's sessions, and Treasury has advised that privacy considerations do factor into the board's decision.

(U) Third, while the Board has an objective and responsibilities, it does not appear to have any explicit authority over CAI or other matters.

4.2.2.2. (U) Department of Homeland Security (DHS). Like the Treasury Department's Data Governance Board charter, the charter for the DHS Data Access Review Council (DARC) could be adapted explicitly to address issues with CAI, and it is our understanding that DHS currently uses the DARC to review bulk CAI acquisitions.

(U) The DARC's members explicitly include representatives from DHS legal, policy, privacy and civil liberties elements.

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

(U//~~FOUO~~) The DARC charter calls for “automatic review” in cases involving an internal or external “bulk data transfer” of PII, and “discretionary review” of other transfers upon the nomination of any DARC member with concurrence of other members, unless the transfer in question has already been approved by higher authority after a review for “legal and policy sufficiency and privacy and civil rights and civil liberties adequacy.”

(U//~~FOUO~~) Highlighting an issue about common use of vocabulary across IC elements, the DARC charter uses “bulk data transfer” to refer to the transfer of “large quantities of intelligence or information, a significant portion of which is not reasonably likely to have any ultimate intelligence or operational value to the recipient.” This is similar to how CIA defines and treats “unevaluated data” (see CIA Guidelines §§ 12.22 (definition) and 6.2 (rules)), as discussed above.

4.2.2.3. (U) [REDACTED] The most mature set of standards and processes governing CAI that we reviewed came from [REDACTED]

(U) Among the documents we saw, these [REDACTED] best represent the kind of end-to-end process for CAI that we think is desirable. [REDACTED]

4.2.3. (U) Assessment of CAI Examples. As the foregoing examples show, there is considerable variation in the approaches to CAI that are currently in effect at IC elements. Some of this variation makes sense in light of varying missions, authorities, and uses for CAI, and much of it is explainable in light of differences in historical experience with CAI. The use of PAI in general, and of CAI in particular, that includes detailed information concerning large numbers of individuals is a relatively new intelligence discipline and still evolving rapidly. We certainly do not mean to say that every IC element must adopt a version of [REDACTED] very detailed procedures. As noted above, however, we think that IC elements should now come together, review best practices and approaches, and adopt standards that reflect their collective experience, as well as the recommendations in this report. We believe that such an effort will result in more uniform (albeit not identical) approaches to CAI across the IC.

(U) Almost all of the IC elements’ acquisition procedures governing CAI that we reviewed are focused on operational and counter-intelligence concerns rather than privacy and sensitivity. To be sure, some of the procedures focus on governance and include legal personnel in decision-making, and some make explicit reference to civil liberties and legal review. But the documents

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

memorializing approaches to CAI do not address privacy and sensitivity with the same level of rigor and focus that they devote to other issues. That leads to our third and final recommendation.

4.3. (U) Recommendation #3: The IC Should Develop More Precise Sensitivity (VPS) Guidance for CAI. As noted above, CAI can include sensitive information with a high volume, proportion, and sensitivity (VPS) of USPI. Many IC elements' guidelines have provisions that are designed to address VPS concerns in the acquisition, retention, and dissemination of information, including but not limited to CAI. We think those VPS provisions are sound and point in the right direction. As set forth in IC guidelines, however, the VPS provisions are general, in the sense that they afford considerable discretion both on when they apply and how they apply (e.g., what they require to protect privacy). We believe that the IC should develop guidance that refines and applies VPS standards more precisely and explicitly to CAI. Again, the guidance and approach need not be identical at each IC element. We discuss immediately below the main issues of structure, process, and substance that we recommend be included in the guidance, and then review and assess three examples of VPS guidance that are currently in effect (or in development) at certain IC elements. Some of the issues discussed here overlap with our second recommendation, discussed above.

4.3.1. (U) Structural and Procedural Issues. In developing VPS guidance for CAI, IC elements should consider, among other things, the following structural and procedural issues:

- (U) Required involvement of relevant parties at all stages, for the most sensitive cases including legal, privacy, and civil liberties personnel within IC elements.
- (U) VPS assessments generally being made prior to acquisition, or at least prior to analytic use of CAI (with a traditional emergency exception allowing prompt post-acquisition assessing and reporting, with an adequate explanation), ideally integrated or coordinated with CAI acquisition reviews discussed in Recommendation #2 (to avoid VPS concerns being raised as an afterthought or too late in the process).
- (U) Approval requirements, with higher levels of approval required for more sensitive cases, including the possibility of approvals by IC element heads in the most sensitive cases.
- (U) Documentation, retention, and availability to relevant personnel of assessments, approvals, and mitigation measures adopted, in keeping with need-to-know and related security principles, to enhance institutional memory.
- (U) Re-evaluation of VPS assessments and measures, both on a regular basis (e.g., annually) and as circumstances change (e.g., in some cases where material, new information sources are added by the vendor to a purchased CAI data set, or significant

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

new uses are found for previously collected CAI). In Recommendation #2, discussed above, we address re-evaluation to address mission needs, a similar process with a different purpose than the re-evaluation discussed here.

- (U) Forwarding of assessments and other documentation to ODNI (and/or other central authorities, such as USDI or elsewhere in DOD), and a formal mechanism for periodic review to allow comparisons and discussion of best practices across IC elements, to inform refinements and other development of new guidance, consistent with need-to-know and related security and counterintelligence requirements.

4.3.2. (U) Substantive Issues. Apart from the structural and procedural issues above, we recommend that IC elements also consider the following substantive issues in developing VPS guidance for CAI:

- (U) Sensitivity of the CAI – e.g., concerning protected constitutional rights (including religion, speech, reading, association, and political activities), precise and persistent location, sexual activity, and embarrassment and risk to USPs if CAI is disclosed, in keeping with the discussion of sensitivity in Part 2 of this report. How do general VPS principles apply in these specific contexts?
- (U) Deanonimization/reidentification issues. To what extent are data that have been anonymized less sensitive if the IC element can, without undue difficulty, reverse the anonymization or otherwise identify individuals?
- (U) Importance of mission served by CAI (to balance against sensitivity of CAI). IC elements should conduct an explicit analysis and balance of sensitivity risks and mission benefits.
- (U) Strength of nexus between CAI and mission, and availability, feasibility, costs, and risks of (less intrusive) alternatives.
- (U) Ability to filter USPI prior to ingestion (e.g., at the vendor or through an intermediary, before it is made available for operational or analytic use at an IC element), recognizing that because the USIC is very likely the only consumer of CAI that would want or need to eschew USPI, this may be inconsistent with covert acquisition.
- (U) Traditional minimization approaches and techniques, including ability to acquire CAI via access to data at the vendor rather than ingestion of data in bulk, limits on retention, access, querying, other use, and dissemination of CAI, and possible requirements for special training of relevant personal and auditing of queries and other uses of CAI.

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

- (U) Availability of other privacy-protective measures in light of the need and anticipated use of CAI (e.g., masking, differential privacy techniques, homomorphic or other forms of encryption) that may not be available or appropriate for all missions and anticipated uses.

4.3.3. (U) Examples of VPS Guidance. Several IC elements have established, or are developing, more refined VPS guidance, including for use with CAI. These efforts also represent a step in the right direction. We review below the approaches taken by three agencies (relevant source materials are in the appendices).

4.3.3.1. (U) DIA. The Defense Intelligence Agency published Procedures for Special Circumstances Collection in DIA Guide 5148.1-2 (February 23, 2021). These procedures provide “guidance to DIA personnel for evaluating whether a collection opportunity should be considered a special circumstances collection.” *Id.* § 2. Where a special circumstances collection is found and authorized, “the collecting DIA element in consultation with [the DIA Office of Oversight and Compliance] must also consider whether enhanced safeguards are required to protect access to the information.” *Id.* § 4.3. Apart from legal and policy restrictions, the following factors are to be considered (*id.* §§ 4.3.1-4.3.5, sub-section numbering omitted):

- (U) Civil liberties and privacy implications of the collection;
- (U) Potential for substantial harm, embarrassment, inconvenience, or unfairness to U.S. persons if the information is improperly used or disclosed;
- (U) Potential future use of the information being retained and the types of queries or searches expected to be conducted;
- (U) Length of time the information will be retained; and
- (U) Practical and technical difficulties associated with implementing any enhanced safeguards.

(U) If enhanced safeguards are deemed necessary under these factors, one or more of the following measures can be used (*id.* §§ 4.4.1-4.4.5, sub-section numbering omitted):

- (U) Procedures for approval for access to and audit of any searches;
- (U) Procedures to restrict access or dissemination including limiting the number of personnel with access or authority to search; establishing a requirement for higher-level approval or legal review before or after access or search; or requiring higher-level approval or legal review before or after U.S. person information is unmasked or disseminated;

~~SECRET~~ / [REDACTED]

~~SECRET~~ / [REDACTED]

- (U) Use of privacy-enhancing techniques, such as information masking that indicates the existence of U.S. person information without providing the content of the information, until the appropriate approvals are granted;
- (U) Use of access controls, including data segregation, attribute-based access, or other physical or logical access methods;
- (U) Additional protective retention measures or training as required.

(U) Before collection occurs (or as soon as possible after it begins, with an explanation of why collection began before authorization and why continued retention of any previously collected information should be authorized), the “DIA collecting element routes a written summary of the results of its evaluation in paragraphs 4.2 through 4.4 ... in a staff package to the appropriate delegated decision authority.” *Id.* § 5. The package is then coordinated with the Office of General Counsel and other appropriate DIA elements. *Id.* If and when collection is approved, OOC notifies the DOD Senior Intelligence Oversight Officer. *Id.* § 6.2.

(U) In addition to agency-specific guidance, it is our understanding that DOD is nearing completion of a Department-wide policy on enhanced safeguards which will impose restrictions on the use of certain sensitive forms of CAI.

4.3.3.2. (~~U//FOUO~~) NSA. The National Security Agency (NSA) adopted NSA/CSS Policy Memorandum 2021-01, Special Circumstances: Guidance for Intelligence Collection of U.S. Person Information, effective for a one-year period beginning March 10, 2021. The NSA memo resembles the DIA Guidance in that it “prescribes the implementation of NSA/CSS procedures for considering whether an intelligence collection opportunity may constitute Special Circumstances Collection requiring enhanced safeguards under paragraph 3.2.e. of” the DOD Manual. NSA Memo ¶ 1. Covered collection opportunities under the NSA memo expressly include those involving information that is “commercially acquired or voluntarily provided,” as well as SIGINT, whenever the information in question “is to be retained in a repository for operational purposes.” *Id.* ¶¶ 1-2. The NSA memo expressly does not apply to “collection decisions regarding individual foreign intelligence targets,” as opposed to, e.g., collection of unevaluated or bulk data; “nor does it apply to analyst queries or disseminations of lawfully collected intelligence information,” or to efforts under NSD 42 to secure U.S. government systems (see DOD Manual § 3.1.a.(3)). *Id.* ¶¶ 1-2. The NSA memo explains that it is not a substitute for consultation with NSA lawyers. *Id.* ¶ 3. All approved Special Circumstances collections are to be reported annually to DOD. *Id.* ¶ 10.

(~~U//FOUO~~) Under the NSA memo, an element of NSA/CSS that is “considering an intelligence collection opportunity” must generally conduct a “Special Circumstances Collection Assessment” (SCCA) “to determine whether [the collection opportunity] includes the

~~SECRET~~ / [REDACTED]

~~SECRET~~ // [REDACTED]

acquisition of USPI that raises special circumstances.” *Id.* ¶ 11. In general, NSA’s guidance emphasizes measures that prevent such acquisition, by requiring that to “the extent practicable, before collection ... organizations will reduce the risk of acquiring USPI that is not responsive to the [mission] purposes of the collection.” *Id.* ¶ 18. The NSA memo explains that “post-collection mitigations do not affect” whether special circumstances are found to exist, but “may affect the appropriate decision level for approval of Special Circumstances Collection.” *Id.* It is clear that NSA would prefer to filter out unnecessary USPI before collection, a laudable goal.

(U) Where USPI cannot be filtered before collection, an SCCA is generally required with respect to CAI and other non-SIGINT collection opportunities but is expressly not required in four defined situations (*id.* ¶ 13.b.):

1) (U) The collection is limited to data or information that is not reasonably anticipated to include USPI, such as statistics or machine-to-machine data (e.g., network infrastructure interactions, netflow, internet routing information);

2) (U) The collection is limited to data or information that is available to the public at large (e.g., telephone listings, technical journals, newspapers, and books), provided that such collection is not reasonably anticipated to include information concerning USPs resulting from negligence or theft (e.g., hacked or stolen data) and is also not reasonably anticipated to include highly sensitive USPI as further described in paragraph 15;

3) (U) The collection is provided with consent of an individual or organization in accordance with [the DOD Manual]; or

4) (U) The collection is not expected to include USPI or is not otherwise governed by [the DOD Manual].

(U) The first two of these four exclusions raise significant questions centered on the application and meaning of the definition of USPI.

[REDACTED]

~~SECRET~~ // [REDACTED]

~~SECRET~~ / [REDACTED]

[REDACTED]

(U//~~FOUO~~) The second exclusion depends largely on how NSA applies the definition of USPI to (publicly available) CAI. The second exclusion generally covers such CAI because it applies to “information that is available to the public at large,” including by paid subscription, but it expressly does not include CAI that is “highly sensitive” as defined in paragraph 15. Thus, under Paragraph 13.b. of the NSA memo, an SCCA is required for the collection of “highly sensitive” CAI (that is not subject to the other exclusions).

(U) The definition of “highly sensitive” in paragraph 15 of the NSA memo refers back to the VPS definition of “special circumstances” in the DOD Manual but develops further the meaning of “sensitivity.” Paragraph 15 explains that the “sensitivity of USPI” depends on “the potential for substantial harm, embarrassment, inconvenience, or unfairness to any USP if the information is improperly used or disclosed,” which is very similar to Section 4.3.2. of the DIA Guidance discussed above, and relevant to some of the concerns raised in Part 2 of this report. Paragraph 15.b.1. of the NSA memo goes on to provide:

(U) Special circumstances exist if the type of information to be collected relates to or aggregates many data types concerning sensitive activities of any identifiable USP. Sensitive activities include political participation, practice of religion, medical information, membership or participation in organizations or associations, financial data, protected speech, location over time, and protected class demographics. Special circumstances also include publicly available data concerning identifiable USPs that the originator did not intend to be made accessible online or otherwise available to the public (e.g., hacked or stolen data).

(U) Standing alone, this language in Paragraph 15.b.1. appears to mean that an SCCA is required, and that sensitive circumstances exist, when NSA collects (a significant volume of) CAI that is “sensitive,” hacked, or stolen USPI (and that is not subject to the other exclusions in paragraph 13.b.).

(U//~~FOUO~~) Under paragraph 15.b.2., special circumstances “do not exist if the type of information to be collected is limited to USPI that people have chosen to share publicly about themselves, unless such information relates to the sensitive activities of any identifiable USP as further addressed above.” As we understand it, NSA does not consider metadata associated

~~SECRET~~ / [REDACTED]

~~SECRET~~ // [REDACTED]

with app downloads or website visits to be data that “people have chosen to share publicly about themselves” within the meaning of this provision. In any case, even if that were not so, paragraph 15.b.2. would require an SCCA, and sensitive circumstances would exist, when NSA collects CAI that includes “sensitive,” hacked, or stolen USPI or that relates to an identifiable USP (again assuming the other exclusions in Paragraph 13.b. do not apply). We are not aware of any further guidance from NSA on this question, although as noted above it is our understanding that NSA is currently working to institute additional compliance guidance regarding the handling of publicly available information. We think it may be helpful for such forthcoming guidance to address these issues explicitly.

(U//~~FOUO~~) Netting out the many layers of guidance in NSA’s memo, as we understand it, much turns on whether information, including “sensitive” CAI, is “USPI” (or information that “relates” to “any identifiable USP”). As discussed above, the first exclusion in Paragraph 13.b. turns expressly on whether machine-to-machine data is determined to contain USPI (and again, our understanding from NSA is that it does not). And the second exclusion ultimately turns on a similar question under paragraph 15.b.1.-2. We believe that further guidance is needed on both issues, and as noted above it may be currently in development.

4.3.3.3. (U//~~FOUO~~) CIA. As of this writing, CIA is in the process of developing principles to govern the acquisition and use of commercial data. [REDACTED]

(U//~~FOUO~~) [REDACTED]

~~SECRET~~ // [REDACTED]

~~SECRET~~ // [REDACTED]

(U//FOUO) [REDACTED]

(U) 4.3.4. Assessment of VPS Examples and Possible Areas of Future Focus. We appreciate and support the effort reflected in the examples reviewed above from DIA, NSA, and CIA. Although VPS guidance for CAI should follow from VPS guidance in general, we believe that CAI presents a sufficiently significant and growing phenomenon to merit specific guidance, as CIA is currently developing in its principles. We support the processes for assessments and approvals in the guidance from DIA and NSA and believe that CIA should develop a similar approach to ensure the proper application of its CAI principles. Although it has made progress, particularly with respect to bulk (or bulky) collection of CAI, further progress needs to be made in developing visibility into and control of the channels through which CIA acquires CAI.

(U) The single most important point, in our view, is that the existing VPS-CAI guidance should be further developed, ideally with examples illustrating the application of standards to cases. We offer four specific areas, drawn from the longer list above, in which such development would be particularly helpful.

(U) First, [REDACTED] some IC elements seem to be embracing a relatively binary model, in which CAI is non-sensitive if the government could and/or historically did overtly and lawfully acquire it directly, and sensitive if the government could not or historically did not do so. Cf. Part 2 of this report. In the former category, for example, would be a database of newspaper and magazine articles, while the latter category would include bulk, persistent cell site location information (CSLI), which would normally require a warrant (under *Carpenter*), or [REDACTED]. This binary model may not satisfactorily classify every possible case involving CAI, but it appears to be at least a good beginning. (As noted above, a third category of CAI, that is not PAI at all because it is available only to governments, is beyond the scope of this report, but worthy of further attention in its own right.) We recommend the IC test and refine the model against the known use cases to develop guidance. Cf. DOD [3115.12](#) (2010). The basic point is that the qualitative nature of CAI may help determine its sensitivity.

(U) Second, in addition to qualitative differences in CAI, quantitative differences are also relevant. CAI that is acquired in bulk will almost always be more sensitive than CAI in smaller data sets. Where bulk acquisition can be avoided, and the volume of acquired data is reduced, it is generally helpful both for intelligence purposes and for the protection of privacy and civil liberties, and it may simplify CAI procedures.

~~SECRET~~ // [REDACTED]

~~SECRET~~ / [REDACTED]

(U) Third, subject to the policy concerns underlying PPD-28's approach to SIGINT, U.S. intelligence law and policy emphasize the protection of USPI, and approaches to CAI should be developed consistent with that emphasis. In general, foreign CAI data sets concerning foreign persons and entities may raise fewer, or at least different, concerns than analogous data sets focused on the United States and/or U.S. persons.

[REDACTED] Fourth, as discussed with respect to the NSA principles, the IC should develop guidance on how the definition of USPI, and the definition of information that pertains to a known USP, apply in the context of CTD and other CAI. If the *New York Times* can easily de-anonymize persistent location data on U.S. persons, and similar efforts are possible and/or may be undertaken by the IC for AdTech and other CAI, is the information therefore USPI? The question arises, and the guidance is needed, because the term USPI is defined in IC policies as "either a single item of information or information that, when combined with other information, is reasonably likely to identify one or more specific U.S. persons," with a recognition that the definition as applied "in a particular context may require a case-by-case assessment by a trained intelligence professional." CIA Guidelines § 12.25; DOD Manual 5240.01 §§ 3.2, G-2. We noted inconsistencies between how different IC elements define and treat USPI, with some treating data as non-USPI because they did not possess other data sets that could be used to reidentify (deanonymize) or because they did not intend to reidentify the individuals in the data. This strikes us as unacceptably narrow; at a minimum, the issue of readily-available deanonymization should be considered closely and more precise guidance provided in the context of CAI.

(U) Beyond these areas, we think that the IC also should at least begin working on assessing and developing more specific guidance for various forms of existing or emerging CAI, including from social media, biometrics, augmented reality/virtual reality (AR/VR), and the Internet of Things.

(U) Even if designed for specific areas, of course, this guidance should be consistent with the principles discussed above.

(U//~~FOUO~~) We are agnostic as to whether the guidance should be set out in a stand-alone document devoted to VPS issues in CAI [REDACTED] added to broader CAI processes (of the sort discussed in our second recommendation above), added as an amendment to existing procedures governing intelligence activities of IC elements, or included in guidance addressing VPS concerns in general (not limited to CAI). The main point is that the guidance be sufficiently clear and specific.

~~SECRET~~ / [REDACTED]

~~SECRET~~ // [REDACTED]

5. (U) CONCLUSION

(U//~~FOUO~~) We tried, in Part 1 of this report, to describe CAI for those who are not already familiar with it. Part 1 therefore included a working definition of CAI (and an explanation of why it is important to define); a list of the main sellers of CAI and a brief description of the types of information they make available; an effort to trace the origins and evolution of CAI in the rise of digital data; and a review of how “anonymized” CAI can be reidentified and linked to individuals.

(U) Part 2 explained why the DNI was right to commission our report. It described how CAI can provide intelligence value and identified several examples of IC contracts for CAI. It also addressed non-analytic uses of CAI and counter-intelligence risks in CAI, and the risks that CAI presents for privacy and civil liberties. As we observed at the end of Part 2, CAI is a relatively new, rapidly growing, and increasingly significant part of the information environment in which the IC must function, deserving of focused attention.

(U) Part 3 reviewed in detail the current IC policy and regulatory framework governing CAI, under which, as information that is available to the general public, it is treated as PAI. Part 3 tried to describe the current state of CAI regulation as a baseline for our recommendations.

(U) Part 4 set out our three main recommendations:

(U) First, the IC should develop a forward-looking and recurring process to catalog the acquisition and use of CAI across its 18 elements. The IC cannot understand and improve how it deals with CAI unless and until it knows what it is doing with CAI.

(U) Second, based on the knowledge gained from that process, the IC should develop a set of adaptable standards and procedures for CAI, governing and requiring regular re-evaluation of acquisition and other decisions. We offer several elements that can be included in those standards and procedures, but also recognize that they will need to be adapted for different IC elements with different CAI missions.

(U) Third, as part of this set of policies and procedures, and/or as a complement to it, the IC should develop more precise sensitivity and privacy-protecting guidance for CAI. Again, we offer several suggestions for the development of such guidance.

(U) If some or all of these recommendations are agreeable, the IC will need a mechanism for putting them into effect, and for making any other changes suggested by continued attention to CAI. One possibility, which we believe is worth considering, would be a traditional working group of IC senior officials. This group would be charged with implementing our recommendations (to the extent approved), sharing best practices, collecting and assessing additional information about the IC's use of CAI, and recommending additional improvements

~~SECRET~~ // [REDACTED]

~~SECRET~~ // [REDACTED]

over time. The group might decide to proceed within the framework of our three recommendations, or it might adopt their substance within a different framework. For example, the working group might focus on developing (1) principles, such as utility, privacy, and quality of data; (2) tools and procedures for implementing those principles, such as technological methods for filtering and limiting data before its ingestion or use; and (3) processes and approval requirements for applying those tools and procedures. As noted above, CAI is both increasingly powerful for intelligence and increasingly sensitive for individual privacy, and while we hope that our 90-day report provides a helpful foundation for developing more refined approaches, we believe that continued efforts will be necessary. We appreciate the opportunity to be of service

~~SECRET~~ // [REDACTED]

~~SECRET~~ // [REDACTED]

6. (U) APPENDICES

6.1. (U) Letter and Terms of Reference

6.2. (U) IC Elements' Materials Governing CAI

6.3. (U) IC Elements' Materials on VPS and/or CAI Collection

~~SECRET~~ // [REDACTED]

EXHIBIT 5

Data Brokers and Sensitive Data on U.S. Individuals

Threats to American Civil Rights, National Security, and Democracy

By Justin Sherman

Overview: This report examines 10 major data brokers and the highly sensitive data they hold on U.S. individuals. It finds that data brokers are openly and explicitly advertising data for sale on U.S. individuals' sensitive demographic information, on U.S. individuals' political preferences and beliefs, on U.S. individuals' whereabouts and even real-time GPS locations, on current and former U.S. military personnel, and on current U.S. government employees. It first describes the problem of virtually unregulated data brokerage in the United States. It then describes the findings of research conducted for this paper on data brokers openly and explicitly advertising sensitive data on U.S. individuals, including a specific analysis of data relating to military personnel. It then concludes with policy implications for the United States—including ways this data collection, aggregation, selling, and sharing threatens civil rights, national security, and democracy.

Author: Justin Sherman is a cyber policy fellow at Duke University's Technology Policy Lab, where he directs the data brokerage research for Duke's Privacy & Democracy Project.

Publication Note: The author's views are their own and also reflect the broader position of the Duke University Sanford Cyber Policy Program. These views do not necessarily represent those of the Duke University Sanford School of Public Policy or Duke University. This paper was produced intellectually independently as part of the data brokerage research team for Duke's Privacy & Democracy Project.¹

Overview of Problem and U.S. Congress Response

Problem: Data brokerage—broadly, the practice of buying, aggregating, selling, licensing, and otherwise sharing individuals’ data—is a virtually unregulated practice in the United States. Major data brokerage firms are presently offering reams of data on U.S. individuals for sale, and virtually nothing in current U.S. law limits their selling that data to a range of actors, from insurance firms to U.S. law enforcement agencies to foreign entities. This data could be used for a range of activities that violate Americans’ civil rights, hurt U.S. national security, and threaten democracy itself.

Data Brokers: There is no single, agreed-upon definition of data brokers in United States law. Vermont and California have their own definitions in state laws that require “data brokers” to register with the state; these laws create a distinction between firms engaged in the general practice of data brokerage (buying, selling, licensing, etc. data) and those that specifically qualify as “data brokers,” which effectively exempts many companies that buy and sell data from complying with the state’s data broker disclosure requirements, because they do not have the narrow “data broker” characteristics. The Federal Trade Commission (FTC) offers its own non-statutory definitions in policy reports, which do not make this same distinction.²

Data Gathering Mechanisms: Data brokers may gather data on individuals directly, from firms they own and/or software applications they control. Data brokers may also purchase, license, or otherwise acquire data second-hand from companies that directly collect this information from their users. They may also crawl government records to develop profiles on individuals (most often seen on “white pages” or “people-search” websites). U.S.-incorporated data brokers often advertise data on U.S. individuals as well as on individuals from many other countries globally.

Data Sharing Mechanisms: Data brokers typically offer pre-packaged databases of information to potential buyers. These databases are packaged along a variety of lines, ranging from the personal preferences and behaviors of the individuals to their specific occupations and roles in society (e.g., military personnel). In addition to outright selling data on individuals, data brokers may also license and otherwise share the data with third parties. There is, at present, limited visibility into data brokerage transaction processes beyond information reported by journalists.

Policy Response: The U.S. Congress should consider giving the executive branch export control authorities to limit potential data broker sales of sensitive data on U.S. individuals to foreign governments and to non-state actors with close ties to foreign intelligence and security agencies. The U.S. Congress should also make data brokerage a central part of robust federal privacy legislation that establishes rules around and implements restrictions on the private collection, aggregation, sale, licensing, and sharing of U.S. individuals’ data—including placing limits on federal government purchasing of data broker data and giving the Federal Trade Commission further authority to investigate unfair and exploitative data broker practices and use of data broker data by other firms.

Research Findings

Overview:

- All 10 surveyed data brokers openly and explicitly advertise data on millions of U.S. individuals, oftentimes advertising thousands or tens of thousands of sub-attributes on each of those individuals, ranging from demographic information to personal activities and life preferences (e.g., politics, travel, banking, healthcare, consumer goods and services)
- People-search websites aggregate public records on individuals and make it possible for anyone to search for major activist figures, senior military personnel, and other individuals—uncovering home address, phone number, and other information as well as the names of known family members and relatives
- Oracle has a data partner that openly and explicitly advertises data on U.S. individuals' interest in political organizations, figures, and causes, including but not limited to data on those who support the National Association for the Advancement of Colored People (NAACP), Planned Parenthood, the American Civil Liberties Union (ACLU), and the National LGBTQ Task Force
- Oracle, Epsilon, and other data brokers openly and explicitly advertise data sharing platforms to which anywhere from dozens to thousands of companies contribute data on individuals
- Multiple data brokers advertise the ability to locate individuals, ranging from the use of driver license records and other aggregated data to pinpointing phone geolocations
- Three major U.S. data brokers, Acxiom, LexisNexis, and Nielsen, openly and explicitly advertise data on current or former U.S. military personnel; LexisNexis advertises a capability to search an individual and identify whether they are active-duty military; and other brokers likely sweep up military personnel in their larger data sets

Data Broker	Headquartered
Acxiom	U.S.
LexisNexis	U.S.
Nielsen	U.S.
Experian	Ireland
Equifax	U.S.
CoreLogic	U.S.
Verisk	U.S.
Oracle	U.S.
Epsilon	U.S.
People-search sites	Many in U.S.

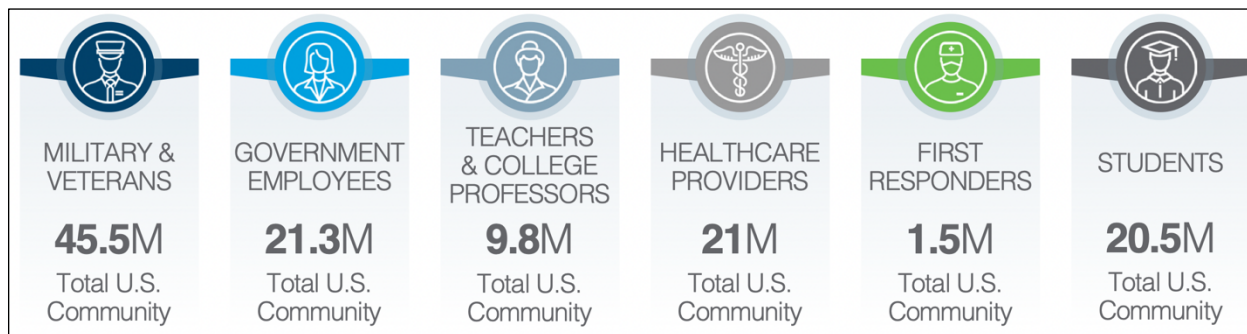
Research Methodology: The author created a list of 10 large data brokers, based on information compiled by research assistants. The author then searched through the publicly available documentation on these data brokers, including promotions and marketing materials on their own public websites, to document their advertising of data on U.S. individuals. The author also wrote a short analysis of people-search websites, based on a survey of multiple major people-search (aka “white pages”) websites. There are many

smaller and potentially less reputable data brokers, but this research focused on the largest, well-known data brokers as well as people-search websites due to their visibility.

—

Acxiom: Broadly, Acxiom advertises data coverage of over 62 countries and the ability to reach over 2.5 billion consumers globally.³ It advertises data attributes on individual demographics (age, gender, ethnicity, education, occupation), household characteristics (household size, number/ages of children), financial data (income ranges, net worth, economic stability), life events (marriage/divorce, birth of children, moves), interests (sports, leisure activities, family, pets, entertainment), buying activities (products bought, method of payment), behavior (community involvement, causes, gaming), major purchases (automotive, home purchase), and geospatial insights (geocoding of latitude/longitude, Census data aggregated at Block, Tract, DMA, ZIP+4).⁴ This data also includes over 225 million landline and wireless telephone numbers in the U.S. and Canada and over 965 million U.S.-based consumer records, including the ability to link emails and names to postal addresses.⁵

Acxiom explicitly advertises data on 45.5 million current and former U.S. military personnel. It advertises a marketing service for clients to send “gated offers” to those individuals, by identifying the intended audience, defining the offer, specifying the channels used for outreach, and establishing the timing of the offer; after this point, Acxiom says it will map out an implementation plan that can go live in as few as 45 days.⁶ Acxiom also offers “verification and location of military servicemen (deployed but missing from base)” as part of commercial work for credit card issuers and retail banks.⁷



Advertisement of Acxiom's data on active and former U.S. military personnel. July 2021.

LexisNexis: LexisNexis advertises data on 270 million transactions around the globe each hour and data linked to over 283 million active U.S. consumer profiles.⁸ It advertises data from 1.5 billion bankruptcy records, 77 million business contact records, 330 million unique cell phone numbers, 11.3 billion unique name and address combinations, 6.6 billion motor vehicle registrations, and 6.5 billion personal property records.⁹ It advertises the ability to “identify relatives, associates and neighbors who may show up in photos or be mentioned in social media postings with a search of hundreds of networks and millions of sites on the open web.”¹⁰ It also advertises the ability to “determine a person’s current whereabouts” using recent driver license records.¹¹

LexisNexis advertises data related to “crime and criminal investigations,” including the ability to “instantly search detailed information using data from over 37 billion public records and 10,000 disparate sources” and the ability to process thousands of records at a time. It advertises the ability to filter and link “billions of records to provide a more complete picture of an individual,” including to “find connections between people and their assets, relatives and business associates.”¹² It advertises customizable alerts of changes to data in an individual’s profile, “state and regional-specific” data sets in addition to public records on individuals, and the ability to, “in minutes, confidently identify, confirm and authenticate identities” for individuals (“especially useful for individuals with common names”).¹³ It says its data sources are updated instantaneously or “as often as every 15 minutes.”¹⁴ Beyond the U.S., it advertises data on individuals in dozens of countries including from “Citizen or National Database information, Credit Header File Information, Electoral Rolls, Property Records, Utility Data and Marketing Sources.”¹⁵ LexisNexis advertises a capability to identify active duty military personnel.¹⁶ It also advertises a Phone Ownership Identification service that “combines robust phone and consumer content with industry-leading identity, relationship and association linking to determine every possible connection between the consumer and phone number provided.”¹⁷

Conduct due diligence – not a scavenger hunt

Imagine if you could simply type in a name and instantly get a report of all people, businesses, assets, civil/criminal matters and other details connected to that individual. Even down to professional licenses and neighboring households.

Advertisement of LexisNexis’ SmartLinx Person Report. August 2021.

Nielsen: Nielsen broadly advertises audience data “across more than 60,000 segments,” including demographics, psychographics, mobile, online, TV, over-the-top TV and audio behavior, spending, store visits, basket size, and product purchases.¹⁸ It advertises purchase history across over 90 million households, in-store purchase data from over 18,000 retail and drug stores, and data from over 2.2 million Universal Product Codes, forming “the largest and most representative [Consumer Packaged Goods] buyer graphic dataset in the U.S.”¹⁹ It advertises data on online and offline transactions across MasterCard, Visa, Discover, and American Express, among others, “representing 80% of all credit card and 30% of all debit card transactions.”²⁰ It also advertises a personality survey on individuals.²¹ It advertises more than 400 data providers—including from Consumer Packaged Goods, travel, shopping, auto, finance, and business-to-business firms—in its Nielsen Marketing Cloud Data-as-a-Service platform.²² Nielsen also explicitly advertises data on current and former U.S. military personnel. It published a report in 2019 on “today’s veteran consumers” that drew on two external sources and four Nielsen data sets, attempting to depict what active and former U.S. military personnel watch, where veterans shop, what veterans spend on what they buy, and how that compares to what the average household buys.²³ Nielsen also advertises its “HomeScan DeCa (Defense Commissary Agency) database” which “tracks consumer

spending at military commissaries and exchanges.”²⁴ The company has publicly published multiple other analyses of U.S. military personnel economic activity that draw on multiple Nielsen surveys and data sets.²⁵

Experian: Experian says it processes over 2 billion records monthly and has over 8 billion name and address combinations, with the ability “to convert sensitive PII [personally identifiable information] data into actionable insights.”²⁶ Experian advertises data on 95% of the U.S. population, including information on 300 million consumers, 126 million living units, and 4.4 billion economic transactions²⁷ spanning thousands of data attributes.²⁸ Experian advertises its ability to “ingest first-party data” such as names, physical addresses, email addresses, mobile ad identifiers (MAIDs), IP addresses, and other information to link economic transactions to “an Experian household ID.”²⁹ It advertises mobile location data on users³⁰ and the ability to link information to 500 million email addresses and 275 million addressable cookies.³¹ The company also advertises services to target individuals using first-party, second-party, or third-party data (terms not defined explicitly on the Experian website, but which likely refer to data a business directly collects on its users (first-party) versus that acquired indirectly (second- and third-party)).³²

Equifax: Equifax advertises data on 45% of the nation’s assets³³ spanning “digital targeting segments” including wealth, financial durability, auto, income, credit card spending propensities, business to business, mortgage, financial mobility, online interest, financial cohorts, investments, insurance, credit card, student loan, retail banking, small business assets, restaurant, ability to pay, communications, travel and leisure, sports, and more.³⁴ It advertises a service for clients to upload their own data on customers, after which Equifax can link the data with its own third-party data for insights.³⁵ It makes claims in multiple marketing documents about “anonymous” data, such as household wealth estimates, but it does not fully elaborate on how “anonymous” is defined nor when anonymization supposedly takes place.³⁶ Journalists have documented how Equifax purchases payroll and employee data from thousands of U.S. businesses;³⁷ Intuit, for instance, recently began sharing the payroll data of 1.4 million businesses with Equifax.³⁸

CoreLogic: CoreLogic advertises data on “more than 99.99% of all properties in the United States.”³⁹ It says that this includes over 1 billion property records sourced and updated annually,⁴⁰ as well as data on property listings, tax records, home valuations, and data related to properties including neighborhoods, flooding, and school data.⁴¹ It says 99.75% of its data “is collected directly from the source.”⁴²

Verisk: Verisk advertises over 22 billion records in commercial and personal lines, “detailed information” on over 6 million commercial properties, insurance fraud data on over 1.4 billion claims, and “depersonalized information” on over 1.8 billion consumer credit, debit, and savings accounts.⁴³ It advertises its “Verisk Data Exchange” that has personal and commercial auto data, connected home data, and claims data, including from auto-makers (Ford, GM, Honda, and Hyundai are listed), telematics service providers (dongles, hardwired aftermarket devices, smartphones, and companies Omnitracs and TomTom are listed), mobile telematics providers, and connected home providers.⁴⁴ For example, it advertises data from over 3.5 million vehicles and on 43 billion miles of driving in its Verisk Data

Exchange.⁴⁵ Verisk identifies several potential sources of smart-home device data for its Data Exchange (though does not specify which are used), including video doorbells, security or surveillance cameras, motion detectors, window/door sensors, flow detectors, water shut-off valves, connected thermostats and temperature sensors, smoke detectors, air particulate detectors, fire detectors, smart appliances and plugs, and electrical panel monitors.⁴⁶ Verisk also advertises a “Reverse Phone Append” feature to get data on an individual “simply by entering their phone number.”⁴⁷

Keep it simple

Enter a phone number on an insurance application, and Reverse Phone Append provides the applicant’s first and last name, street address, city, state, and ZIP code.

Advertisement of Verisk’s “Reverse Phone Append” service. July 2021.

Oracle: Oracle advertises partnerships with over 74 other data providers accessible to clients through the Oracle BlueKai marketplace.⁴⁸ For example, Affinity Answers, one of the partner data providers, advertises data on billions of consumer engagements.⁴⁹ Affinity Answers advertises data on individuals’ preferred stores, e-commerce websites, video streaming sites, internet service providers, cellular service providers, consumer products, television shows, podcast genres, sports teams, travel vendors (airlines, cruises, car rental services, etc.), and financial service firms (spanning banking and insurance). Affinity Answers also advertises data on individuals’ interests in political organizations (e.g., NAACP, National LGBTQ Task Force, Planned Parenthood), political media figures (e.g., Bill O’Reilly, Glenn Beck, Anderson Cooper, Arianna Huffington), state-level Democratic Party and Republican Party organizations, and specific politicians in office.⁵⁰ Oracle has also purchased many data broker firms, such as Bluekai and Datalogix in 2014; at the time of purchase, Datalogix advertised data from 1,500 “data partners” that covered \$2 trillion in consumer spending across 110 million households.⁵¹ Oracle does not explicitly advertise data on current or former U.S. military personnel, but it provides data from Acxiom through its Oracle BlueKai marketplace, and Acxiom explicitly advertises data on U.S. military personnel (see above).

Epsilon: Epsilon advertises “vital data” on 250 million U.S. consumers, composed of over 7,000 attributes on each consumer, including transaction data and online behavior.⁵² It also advertises millions of cross-device IDs.⁵³ It advertises its “Abacus Alliance,” which it calls “the largest cooperative database in the U.S.,” where more than 3,000 companies contribute data on individuals;⁵⁴ every week, Epsilon says, over 250 “multi-channel brands” upload customer transactional data, including what individuals purchased, when, where, and for

how much money.⁵⁵ It advertises sourcing records from public records (including voter registration files, phone books, deeds, and permits), surveys (“self-reported data from 20 million households”), partners (data from corporate sources), and “multi-sourced” information, which it describes as “real transactional data” on categories of purchases.⁵⁶

Other—People-Search Websites: “People-search websites,” commonly referred to as “white pages” websites, allow internet users to search for information on an individual by entering their name. These websites typically scrape this information from public records (property records, tax filings, voting records, etc.), aggregate it, and publish it online in a searchable format; these searches may be free-of-charge or run for a small fee. People-search websites cover much of the U.S. population, and as such, it is highly likely that, for example, many active and former U.S. military personnel’s address, contact, and family information is searchable via these publicly available websites. The author was able to conduct searches on multiple, unnamed, publicly accessible people-search websites that appeared to provide data (e.g., phone numbers, address information) for senior members of the U.S. military. The same could be done for any number of activists or other individuals who are at higher risk of being targeted with violence by domestic organizations.

Analysis of Policy Implications for the United States

Threats to Civil Rights:

U.S. federal agencies from the Federal Bureau of Investigation (FBI) to U.S. Immigration and Customs Enforcement (ICE) purchase data from data brokers—without warrants, public disclosures, or robust oversight—to carry out everything from criminal investigations to deportations.⁵⁷ In doing so, data broker companies circumvent limits on companies directly handing data to law enforcement (e.g., a cellular company can sell user data to a data broker which can then sell the data to the FBI). The federal government agencies using the data may then also circumvent a variety of legal restrictions in place around searches and seizures as well as federal controls which are not applied to “open source” or “commercially obtained” data, even if the data is on U.S. individuals.

Data brokers also hold highly sensitive data on U.S. individuals such as race, ethnicity, gender, sexual orientation, immigration status, income level, and political preferences and beliefs (like support for the NAACP or National LGBTQ Task Force) that can be used to directly undermine individuals’ civil rights. Even if data brokers do not explicitly advertise these types of data (though in many cases they do), everything from media reporting to testimony by a Federal Trade Commission commissioner has identified the risk that data brokers use their data sets to make “predictions” or “inferences” about this kind of sensitive information (race, gender, sexual orientation, etc.) on individuals.⁵⁸

This data can be used by commercial entities within the U.S. to discriminately target goods and services, akin to how Facebook advertising tools allow advertisers to exclude certain groups, such as those who are identified as people with disabilities or those who are identified as Black or Latino, from seeing advertisements.⁵⁹ Many industries from health insurance to life insurance to banking to e-commerce purchase data from data brokers to run advertisements and target their services. A 2018 ProPublica investigation, for example, found that health insurers were purchasing data from data brokers (including data on individuals’ race, marital status, education level, net worth, TV consumption, and whether bills are paid on time) to predict health costs.⁶⁰ Given identified discrimination problems in machine learning algorithms, there is great risk of these predictive tools only further driving up costs of goods and services (from insurance to housing) for minority groups. Data on military personnel has also been used for exploitative commercial purposes, as with for-profit schools using acquired data to target predatory advertisements or outright scams to veterans looking for educational opportunities.⁶¹

Companies are not required to inform individuals that they are being micro-targeted with advertisements using this data. Consumers do not necessarily know that the data about them is being collected; nor in most cases do they have legal recourse to have the data corrected by a data broker if it is inaccurate (e.g., incorrectly logging a felony conviction).⁶² The last of these possibilities is not hypothetical: a 2020 investigation by The Markup identified dozens of cases in which Americans were denied housing because of mistakes in criminal record data—data which the companies in question often acquired from data brokers or people-search websites.⁶³

Data brokers' troves of data on U.S. individuals also pose threats to civil rights from the government side. Given a long history of American law enforcement exclusively or disproportionately targeting marginalized individuals and communities with surveillance,⁶⁴ there is also great risk that data points on individuals' race, ethnicity, gender, sexual orientation, immigration status, and other demographic characteristics will be used in discriminatory policing and surveillance. This data could also be acquired, without a warrant, for law enforcement use in training artificial intelligence surveillance tools. It could also be outright wrong: a 2019 ruling by a U.S. district court in California found that "[t]he databases on which ICE relies for information on citizenship and immigration status often contain incomplete data, significant errors, or were not designed to provide information that would be used to determine a person's removability."⁶⁵

Data brokers could also be hacked—especially where data brokers do not adequately invest in cybersecurity—and sensitive data on U.S. individuals could be publicly leaked in damaging ways. For example, data broker Social Data in 2020 was found to have an unsecured, non-password-protected database facing the public internet with data on 235 million social media profiles, all due to a database configuration error.⁶⁶

And individuals can use this data held by data brokers to discriminate against others as well. The Catholic website The Pillar recently outed a gay priest by purchasing data on the individual's Grindr usage (including location data) from a third party that obtained it from the app.⁶⁷ This will not be the last time an individual's location data was acquired by a third party intent on inflicting harm. Members of vulnerable communities may not be aware that their data is widely collected, aggregated, and sold to whomever is buying, such as with LGBTQ individuals using dating apps and sharing their GPS location, sexual preferences, sexual health statuses, and more. Research from Duke's Cyber Policy and Gender Violence Initiative has also identified numerous ways in which abusive individuals can use people-search websites to obtain data broker data to carry out stalking, harassment, and physical violence against intimate partners—violence which is overwhelmingly directed at women and members of the LGBTQ community.⁶⁸ Privacy is quite literally, as the Cyber Policy and Gender Violence Initiative says, a matter of life and death for survivors of domestic violence, yet data broker websites can publish and sell information on an individual's address with no restrictions. Individuals could similarly obtain information about activists, political organizers, and other people for the purposes of violence, intimidation, or harassment as well.

Threats to National Security:

Three of the 10 data brokers surveyed for this report—Acxiom, LexisNexis, and Nielsen—openly and explicitly advertise data on current and/or former U.S. military personnel. LexisNexis identifies a capability to specifically identify active U.S. military personnel. Data sets on U.S. military personnel are not necessarily used for nefarious purposes: current and former U.S. military personnel are a unique demographic, and as such, many different industries may want to target them with uniquely tailored advertisements for products and services. It is also possible some data brokers may offer economic opportunities through the

use of this information without actually selling the information to a client—e.g., allowing a client insurance firm to run ads through the data broker’s platform, but without ever handing over the underlying data on particular individuals.

That said, many data brokers actively sell their data sets to willing buyers. There is little transparency, if any at all, into data brokerage transactions. There is also virtually nothing in U.S. law preventing data brokers from selling information on U.S. individuals to foreign entities. The data advertised by these brokers—spanning everything from financial transaction histories and internet browsing patterns to travel interests and support for political causes and organizations—could be used by foreign entities for a range of national security-damaging activities. This could include building profiles on senior U.S. military personnel involved in key decisions relevant to a foreign power, or even building profiles on their family members and close acquaintances (seeing as some data brokers openly and explicitly advertise their ability to map network connections between individuals), for the purposes of information operations, coercion, blackmail, or intelligence-gathering. Should terrorist organizations acquire any of this data broker data on U.S. military personnel, the consequences could potentially even be more dire. As mentioned, there are few mechanisms in place for the U.S. government to limit the sharing of data brokerage data, including highly sensitive data, on U.S. individuals. Buyers of data broker data could potentially combine data from multiple brokers together to, for example, uncover a U.S. military or government employee’s family member and then obtain their real-time location and/or location history.

More broadly, the data on U.S. individuals held by data brokers is highly sensitive and could be used in many other ways to undermine U.S. national security. Foreign actors, such as Russia’s Internet Research Agency, could use this data to bolster their influence campaigns to interfere in U.S. electoral processes. Criminal organizations could use this data to build profiles on and subsequently target prosecutors and judges. Foreign intelligence organizations could acquire this data through a variety of means—including through front companies that could legally purchase the data from U.S. brokers, and through simply hacking a data broker and stealing it all—to build profiles on politicians, media figures, diplomats, civil servants, and even suspected or secretly identified intelligence operatives.

Threats to Democracy:

Data on U.S. individuals shared and/or sold by U.S. data brokers could be used for activities that specifically threaten elements of the U.S. democratic electoral system, such as by foreign governments micro-targeting individuals with election disinformation intended to sow chaos or dissuade voter participation (e.g., as the Russian Internet Research Agency did to Black communities in 2016)⁶⁹ or by domestic terror organizations carrying out voter intimidation and suppression. For example, there is virtually nothing in U.S. law preventing data brokers from selling highly sensitive political preference information on millions of U.S. individuals to foreign entities. Political campaigns in the United States already purchase data broker data to plan and execute their outreach to U.S. voters, though voters have little visibility into the details of this practice.⁷⁰

Broadly, the data brokerage ecosystem represents the unrestrained aggregation of surveillance power as a service. Companies openly and explicitly advertise immense data sets on U.S. individuals with thousands of sub-attributes that reveal highly sensitive behavior—from marketing materials that detail information on individuals’ economic activity and health provider preferences to a company advertising a tool to search anyone’s phone number and return a name, address, and other information (which can then be used for subsequent data-searching). Federal law enforcement agencies purchase information from data brokers in a manner that has the impact of circumventing protections against acquiring and using data on U.S. individuals; companies use data brokers to develop “predictive” models on consumers and to discriminately target goods and services; and individuals are increasingly using data brokers to inflict harm on vulnerable communities and specific other individuals. Entities that purchase or otherwise acquire data from multiple brokers—again, a practice that is virtually unregulated in the United States—would have an even larger, more intimate, and consequently more dangerous data set. The purchasing of detailed data sets on military personnel is an illustrative example of business practices that do not have sufficient oversight or accountability.

Conclusion:

There are virtually no controls on the data brokerage industry (data broker firms specifically) and on the practice of data brokerage itself (the broader buying, licensing, and sharing of data that underpins these companies’ operation). Americans also do not have federal privacy rights to gain insight into the data brokerage ecosystem’s surveillance of them, nor do they have federal rights to demand that incorrect data is corrected;⁷¹ federal enforcement agencies like the Federal Trade Commission, conversely, do not have a strong federal privacy law to point to as grounds to investigate unfair and exploitative practices by data brokers and by firms using data broker data. All these harms—to Americans’ civil rights, to U.S. national security, and to U.S. democracy writ large—will only persist without further regulation.

Endnotes

¹ For complete disclosure of funders of the Duke University Sanford Cyber Policy Program, see the External Relationships section of <https://scholars.duke.edu/person/David.Hoffman>. No specific direct funding was provided for this report, and no funders reviewed any of this research before publication or had any editorial control over the report's substantive content.

² Justin Sherman, "Federal Privacy Rules Must Get 'Data Broker' Definitions Right," *Lawfare*, April 8, 2021, <https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right>.

³ Acxiom, *Global Data Navigator*, https://www.acxiom.com/wp-content/uploads/2018/03/Fact_Sheet_Global_Data_Navigator.pdf, 2.

⁴ Acxiom, *InfoBase*, <https://www.acxiom.com/wp-content/uploads/2020/07/ac-2490-19-fs-acxiom-infobase.pdf>, 1.

⁵ *Ibid.*, 2.

⁶ Acxiom, *Gated Offers*, https://www.acxiom.com/wp-content/uploads/2020/07/AC-0991-20_Collateral_Fact_Sheet_Gated_Offers_-_GENERIC_Final_5-19-20.pdf.

⁷ Acxiom, *Government Capability Statement*, <https://www.acxiom.com/wp-content/uploads/2019/11/government-capability-statement-fact-sheet-9-24-19.pdf>, 2.

⁸ LexisNexis, "Our Technology," Risk.LexisNexis.com, <https://risk.lexisnexis.com/our-technology>; LexisNexis, "Public Records," Risk.LexisNexis.com, <https://www.lexisnexis.com/en-us/products/public-records.page>.

⁹ LexisNexis, "Search Public Records," Risk.LexisNexis.com, <https://www.lexisnexis.com/en-us/products/public-records/powerful-public-records-search.page>.

¹⁰ *Ibid.*

¹¹ LexisNexis, "Up to 1 million new records daily," Risk.LexisNexis.com, <https://www.lexisnexis.com/en-us/products/public-records/dynamic-continuously-updated-collection.page>.

¹² LexisNexis, "Crime and Criminal Investigation Solutions," Risk.LexisNexis.com, <https://risk.lexisnexis.com/law-enforcement-and-public-safety/crime-and-criminal-investigations>.

¹³ *Ibid.*

¹⁴ LexisNexis, "Law Enforcement Data, Analytics & ID Linking," Risk.LexisNexis.com, <https://risk.lexisnexis.com/law-enforcement-and-public-safety>.

¹⁵ LexisNexis, "Instant Verify International," Risk.LexisNexis.com, <https://risk.lexisnexis.com/global/en/products/instant-verify-intl-global>.

¹⁶ LexisNexis, "Collections Compliance," Risk.LexisNexis.com, <https://risk.lexisnexis.com/collections-and-recovery/collections-compliance>.

¹⁷ *Ibid.*

¹⁸ Nielsen, "Nielsen Data As a Service," Nielsen.com, <https://www.nielsen.com/us/en/solutions/capabilities/nielsenmarketingcloud-daas/>.

¹⁹ *Ibid.*

²⁰ *Ibid.*

²¹ *Ibid.*

²² *Ibid.*

²³ Nielsen, *Beyond the Uniform*, <https://www.nielsen.com/wp-content/uploads/sites/3/2019/07/beyond-the-uniform-a-look-at-todays-veteran-consumers.pdf>.

²⁴ Nielsen, "Serving Today's Military Consumers," Nielsen.com, November 4, 2014, <https://www.nielsen.com/us/en/insights/article/2014/serving-todays-military-consumers/>.

²⁵ See, e.g., Nielsen, "Connecting with Women in the Military," Nielsen.com, May 17, 2016, <https://www.nielsen.com/us/en/insights/article/2016/connecting-with-women-in-the-military/>; Nielsen, "Roger That: Reaching Today's Military Consumers," Nielsen.com, November 10, 2014, <https://www.nielsen.com/us/en/insights/article/2014/roger-that-reaching-todays-military-consumers/>.

²⁶ Experian, "OmniView," Experian.com, accessed July 2020, <https://www.experian.com/marketing-services/omniview>.

²⁷ Experian, *ConsumerView: Data by the Numbers*, <https://www.experian.com/content/dam/marketing/na/assets/ems/marketing-services/documents/infographics/consumerview.pdf>.

-
- ²⁸ Experian, *ConsumerView*, <https://www.experian.com/content/dam/marketing/na/assets/ems/marketing-services/documents/brochures/consumerview-brochure.pdf>, 3.
- ²⁹ Experian, *OmniImpact*, <https://www.experian.com/content/dam/marketing/na/assets/ems/marketing-services/documents/product-sheets/omniimpact.pdf>, 1.
- ³⁰ *Ibid.*
- ³¹ Experian, *ConsumerView: Data by the Numbers*.
- ³² Experian, *ConsumerView*, 8.
- ³³ Equifax, “Why Equifax?” DataDrivenMarketing.Equifax.com, <https://datadrivenmarketing.equifax.com/why-equifax/overview/>.
- ³⁴ Equifax, “Digital Targeting Segments,” DataDrivenMarketing.Equifax.com, <https://datadrivenmarketing.equifax.com/digital-targeting-segments/>.
- ³⁵ Equifax, “Overview of Services,” DataDrivenMarketing.Equifax.com, <https://datadrivenmarketing.equifax.com/capabilities/overview/>.
- ³⁶ See, e.g., Equifax, *WealthComplete Household Direct Digital*, URL, 3; Equifax, *Digital Targeting Segments: Online Interest*, https://resources.datadrivenmarketing.equifax.com/digital-marketing/digital-targeting-segments-online-interest?_ga=2.222403995.1491988852.1625766298-1515325844.1625671484, 1, 2.
- ³⁷ Jennifer Surane, “Equifax Amassed Salary Details for People at 7,100 Companies,” *Bloomberg*, October 2, 2017, <https://www.bloomberg.com/news/articles/2017-10-02/equifax-has-amassed-salary-details-for-people-at-7-100-companies>.
- ³⁸ Brian Krebs, “Intuit to Share Payroll Data from 1.4M Small Businesses With Equifax,” *Krebs on Security*, July 1, 2021, <https://krebsonsecurity.com/2021/07/intuit-to-share-payroll-data-from-1-4m-small-businesses-with-equifax/>.
- ³⁹ CoreLogic, “Property Data Solutions,” CoreLogic.com, <https://www.corelogic.com/find/property-data-solutions/>.
- ⁴⁰ CoreLogic, “Gold Standard Data & Property Solutions,” CoreLogic.com, <https://www.corelogic.com/why-corelogic/>.
- ⁴¹ CoreLogic, “The Benefits of Trestle” (video) on “Trestle,” Trestle.CoreLogic.com, <https://trestle.corelogic.com/Home/AssertionConsumer/Brokers>.
- ⁴² CoreLogic, “Gold Standard Data.”
- ⁴³ Verisk, “Verisk Analytics Fact Sheet,” Verisk.com, <https://www.verisk.com/verisk-in-the-news/verisk-analytics-fact-sheet/>.
- ⁴⁴ Verisk, “The Verisk Data Exchange,” Verisk.com, <https://www.verisk.com/insurance/products/telematics/>.
- ⁴⁵ Saurabh Khemka, “Omnitracs to join Verisk Data Exchange,” Verisk.com, June 14, 2018, <https://www.verisk.com/insurance/visualize/omnitracs-to-join-verisk-data-exchange/>.
- ⁴⁶ Sandra Maples, “How smart devices are providing the data claims professionals need,” Verisk.com, October 3, 2017, <https://www.verisk.com/insurance/visualize/how-smart-devices-are-providing-the-data-claims-professionals-need/>.
- ⁴⁷ Verisk, “Reverse Phone Append,” Verisk.com, <https://www.verisk.com/insurance/products/reverse-phone-append/>.
- ⁴⁸ Oracle Audiences,” Oracle.com, <https://www.oracle.com/cx/advertising/audiences/>; “Branded Data Providers,” Oracle.com, <https://www.oracle.com/cx/advertising/data-providers/>.
- ⁴⁹ “Social Insights-Powered Audiences,” AffinityAnswers.com, <https://www.affinityanswers.com/programmatic-display/>.
- ⁵⁰ Affinity Answers Syndicated Taxonomy, June 2020 (Excel file), downloaded from “Social Insights-Powered Audiences.”
- ⁵¹ “Oracle Buys Datalogix,” Oracle.com, December 22, 2014, <https://www.oracle.com/corporate/pressrelease/oracle-buys-datalogix-122214.html>.
- ⁵² “Understand your customer analytics with consumer data,” Epsilon.com, <https://www.epsilon.com/us/products-and-services/data>; “Financial Services Digital Marketing Solutions,” Epsilon.com, <https://www.epsilon.com/us/industries/financial-services>.
- ⁵³ “Power of Me,” Epsilon.com, <https://us.epsilon.com/power-of-me>.
- ⁵⁴ “Understand your customer analytics.”
- ⁵⁵ “Direct mail success with Epsilon’s Abacus Alliance,” Epsilon.com, <https://www.epsilon.com/abacus/the-abacus-alliance>.

⁵⁶ “Do more with your data to drive better outcomes,” Epsilon.com, <https://www.epsilon.com/us/products-and-services/data>.

⁵⁷ See, e.g., Sara Morrison, “A surprising number of government agencies buy cellphone location data. Lawmakers want to know why,” *Recode*, December 2, 2020, <https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel>; Joseph Cox, “CBP Bought ‘Global’ Location Data from Weather and Game Apps,” *VICE*, October 6, 2020, <https://www.vice.com/en/article/n7wakg/cbp-dhs-location-data-venntel-apps>; Drew Harwell, “ICE investigators used a private utility database covering millions to pursue immigration violations,” *The Washington Post*, February 26, 2021, <https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/>.

⁵⁸ See, e.g., among many others, Thorin Klosowski, “Big Companies Harvest Our Data. This Is Who They Think I Am,” *The New York Times*, May 28, 2020, <https://www.nytimes.com/wirecutter/blog/data-harvesting-by-companies/>; “Data Brokers: A Call for Transparency and Accountability,” Statement of Commissioner Julie Brill, Federal Trade Commission, May 27, 2014, https://www.ftc.gov/system/files/documents/public_statements/311551/140527databrokerrptbrillstmt.pdf.

⁵⁹ This was the subject of a U.S. Department of Housing and Urban Development complaint in 2018: “US regulators target Facebook on discriminatory housing ads,” Associated Press, August 17, 2018, <https://apnews.com/article/north-america-lawsuits-us-news-real-estate-brokers-tx-state-wire-f02eb72214ac43638ba1a5ab6daea4e8>. A July 2021 investigation by *The Markup* found that Facebook still uses many proxies for categories like race in its advertising tools: Jon Keegan, “Facebook Got Rid of Racial Ad Categories. Or Did It?” *The Markup*, July 9, 2021, <https://themarkup.org/citizen-browser/2021/07/09/facebook-got-rid-of-racial-ad-categories-or-did-it>.

⁶⁰ Marshall Allen, “Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates,” *ProPublica*, July 17, 2018, <https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates>.

⁶¹ See, e.g., *Private For-Profit Colleges and Online Lead Generation* (Washington, D.C.: Center for Digital Democracy, May 2015), https://www.democraticmedia.org/sites/default/files/field/public-files/2015/forprofitcollegeleadgenreport_may2015_uspirgef_cdd_0.pdf; “The Predatory Underworld of Companies that Target Veterans for a Buck,” Student Borrower Protection Center, <https://protectborrowers.org/the-predatory-underworld-of-companies-that-target-veterans-for-a-buck/>.

⁶² Fair Credit Reporting Act protections are an exception, but the individual’s rights are limited to just specific uses of the data by the data broker.

⁶³ Lauren Kirchner, “When Zombie Data Costs You a Home,” *The Markup*, October 6, 2020, <https://themarkup.org/locked-out/2020/10/06/zombie-criminal-records-housing-background-checks>.

⁶⁴ See, e.g., Alvaro Bedoya, “The Color of Surveillance,” *Slate Magazine*, January 28, 2016, <https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html>; Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Durham: Duke University Press, 2015).

⁶⁵ Joan Friedland, “How the Trump Deportation Machine Relies on Inaccurate Databases and Unregulated Data Collection,” National Immigration Law Center, November 1, 2019, <https://www.nilc.org/2019/11/01/inaccurate-data-unregulated-collection-fuel-deportation-machine/>.

⁶⁶ Scott Ikeda, “Major Data Broker Exposes 235 Million Social Media Profiles in Data Leak,” *CPO Magazine*, August 28, 2020, <https://www.cpomagazine.com/cyber-security/major-data-broker-exposes-235-million-social-media-profiles-in-data-leak/>.

⁶⁷ “Priest outed via Grindr app highlights rampant data tracking,” NBC News, July 22, 2021, <https://www.nbcnews.com/tech/security/priest-outed-grindr-app-highlights-rampant-data-tracking-rcna1493>.

⁶⁸ “Privacy Issues from Data Brokers,” Duke Cyber Policy and Gender Violence Initiative, <https://sites.sanford.duke.edu/genderviolencepolicy/privacy-issues-for-gender-violence-survivors/>; “Domestic Violence and the LGBTQ Community,” National Coalition Against Domestic Violence, June 6, 2018, <https://ncadv.org/blog/posts/domestic-violence-and-the-lgbtq-community>.

⁶⁹ Jason Parham, “Targeting Black Americans, Russia’s IRA Exploited Racial Wounds,” *WIRED*, December 17, 2018, <https://www.wired.com/story/russia-ira-target-black-americans/>.

⁷⁰ Geoffrey A. Fowler, “How politicians target you: 3,000 data points on every voter, including your phone number,” *The Washington Post*, October 27, 2020,

<https://www.washingtonpost.com/technology/2020/10/27/political-campaign-data-targeting/>; Jeremy B. Merrill, “How to Wrestle Your Data From Data Brokers, Silicon Valley — and Cambridge Analytica,” ProPublica, April 30, 2018, <https://www.propublica.org/article/how-to-wrestle-your-data-from-data-brokers-silicon-valley-and-cambridge-analytica>.

⁷¹ Some narrow rights may apply with respect to certain categories of data, such as children’s data or clinical health data, or data uses, such as credit reporting.

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

PROJECT FOR PRIVACY AND
SURVEILLANCE ACCOUNTABILITY, INC.,

Plaintiff,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

No. 1:22-cv-1812-RC

[PROPOSED] ORDER

Upon consideration of Plaintiff's cross-motion for summary judgment and opposition to Defendants' motion for summary judgment, and the entire record herein, it is hereby:

ORDERED that Defendants' motion for summary judgment is DENIED; and it is

FURTHER ORDERED that Plaintiff's cross-motion for summary judgment is GRANTED, and judgment is entered in Plaintiff's favor.

SO ORDERED.

Date

U.S. District Judge