UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

SUSAN B. LONG and DAVID BURNHAM, Plaintiffs, v. IMMIGRATION AND CUSTOMS ENFORCEMENT and CUSTOMS AND BORDER PROTECTION Defendants.	)	Civil Action No. 1:14-cv-109 (APM)

REPLY MEMORANDUM IN SUPPORT OF
PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT

Scott L. Nelson
DC Bar No. 413548
PUBLIC CITIZEN LITIGATION GROUP
1600 20th Street NW
Washington, DC 20009
(202) 588-1000

Counsel for Plaintiffs

March 30, 2015

INTRODUCTION

The technical issues involved in this case should not obscure what is at stake. The defendant agencies possess databases containing large quantities of non-exempt information about their enforcement proceedings, constituting the "official records" of their activities. Patterson Dec., Exh. A, at 6 (Doc. 18-1). Such databases are agency records, which FOIA requires the government to make available, in electronic form if so requested, with any exempt information segregated and redacted. The agencies here attempt to render that requirement meaningless by withholding basic information necessary to make the databases intelligible: information about their structure, including the tables they contain and the fields of information within those tables, without which the databases are meaningless gibberish.

As to the requested excerpts of the databases themselves, the government contends that although much or most of what they contain is non-exempt, copying them would create "new records," which FOIA does not require. The government further argues that the volume of information is a reason not to copy it or segregate non-exempt and exempt information, even though readily available electronic processes render both copying large quantities of data and redacting it a largely mechanical matter, and other agencies routinely use such processes to produce comparably large and complex databases containing both information subject to disclosure and exempt information requiring redaction.

The arguments the government advances to negate its obligations to produce electronic information in a meaningful manner lack both a legal and factual basis.

The government posits speculative risks attributable not to the production of the requested information itself, but to unlikely breakdowns in the agency's data security—risks that are not within the scope of the exemptions claimed. The agency's new Exemption 3 argument is based on a repealed statute that has been replaced by one that, on its face, does not satisfy Exemption 3 and disclaims any effect on agency obligations under FOIA. And the argument that copying the requested snapshots of database tables would constitute creation of new records is directly contrary to FOIA's requirement that agencies make records available in electronic formats sought by requesters—a requirement that excludes the argument that requiring an agency to copy electronic records into different formats is impermissible under FOIA.

ARGUMENT

I. ICE has failed to support its Exemption 7(E) claims.

A. The requested information about the databases does not disclose investigative or prosecutorial methods.

The databases that are the subjects of the FOIA requests at issue contain information about ICE and CBP proceedings. The government has invoked Exemption 7(E) to withhold not the *contents* of the databases, but information about their *structure*. That the databases themselves may contain information compiled for law enforcement purposes does not, as the government assumes, mean that all information *about* the databases—especially information that, like the information requested here, serves data management and administrative purposes—was also compiled for law enforcement purposes, the threshold requirement under Exemption 7. *See Pratt v. Webster*, 673 F.2d 408, 420–21 (D.C. Cir. 1982); *Am. Immigration*

Council v. U.S. Dept. of Homeland Sec., 950 F. Supp. 2d 221, 245–46 (D.D.C. 2013). Moreover, Exemption 7(E) exempts not law enforcement records generally, but only those whose release would "disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions." 5 U.S.C. § 552(b)(7)(E). ICE has failed to show that releasing information about its databases would disclose investigative or prosecutorial techniques, procedures, or guidelines.

ICE's declarations do not demonstrate that the records plaintiffs requested set forth, describe, or identify investigative or prosecutorial techniques, procedures or guidelines.[1] Rather, ICE relies on a false syllogism: It asserts that because ICE "employed certain law enforcement techniques and methods" to *obtain* the information in the databases, and because ICE law enforcement personnel *use* that information to "carry out [their] duties," it follows that release of information about the databases' structure would disclose the techniques and methods that led to collection of the data or that ICE law enforcement officers employ when they use it. ICE Opp.-Reply, at 4–5. ICE goes so far as to assert—wrongly—that by agreeing that the information in the databases relates to ICE proceedings, plaintiffs have "concede[d] that the information in the subject databases would disclose techniques,

[1] *See Citizens v. Responsibility & Ethics in Wash. v. U.S. Dept. of Justice*, 746 F.3d 1082, 1101–02 (D.C. Cir. 2014) ("*CREW*") (agency must explain how disclosure would reveal investigative procedures); *Am. Immigration Council,* 950 F. Supp. 2d at 246–47 (same).

procedures, and guidelines for law enforcement as well as information regarding current and past investigations." *Id*. at 5.

The flaw in ICE's reasoning is obvious: Revealing information about proceedings that result from the use of law enforcement techniques and methods is not the same as disclosing those techniques and methods. For example, disclosing that someone has been arrested, booked, detained, or removed does not reveal the techniques that led to the arrest, booking, detention or removal or the guidelines that the agency followed that led to the proceedings. *See Judicial Watch, Inc. v. U.S. Secret Serv.*, 579 F. Supp. 2d 182, 187–88 (D.D.C. 2008). Revealing information about the structure of the databases that contain information about such proceedings is even further removed from disclosure of the underlying investigative and prosecution techniques and methods. And the fact that data is used by law enforcement personnel in carrying out their duties does not mean that revealing information about a database discloses the techniques and methods that law enforcers employ in using it.[2]

Because ICE has not provided any evidence that disclosing information such as the names of tables within the databases and the fields of information they contain would reveal investigative or prosecutorial techniques, procedures, and guidelines, it has failed to make a threshold showing that Exemption 7(E) applies.

[2] This case is unlike *Cozen O'Connor v. U.S. Dept. of Treasury*, 570 F. Supp. 2d 749, 786 (E.D. Pa. 2008), in which the requested information would have revealed *how* law enforcement officers used data in investigations, and *Blackwell v. FBI*, 646 F.3d 37 (D.C. Cir. 2011), where the information concerned techniques for forensic examination of computers and the methods of collecting data in investigative reports.

B. The "circumvention" ICE posits would not result from disclosure of investigative or prosecutorial methods.

Exemption 7(E) requires not only that the government show that release of records would disclose investigative or prosecutorial techniques, procedures, and guidelines, but also that "*such disclosure* could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E) (emphasis added). Thus, the exemption applies only when the anticipated circumvention is attributable to the *disclosure of the law enforcement methods* identified in Exemption 7(E), not just when disclosure of information might be useful in some way to someone who might violate the law, or even when disclosure of information compiled for law enforcement purposes might aid a potential lawbreaker. *See Milner v. Dept. of Navy*, 562 U.S. 562, __, 131 S. Ct. 1259, 1267–68 (2011). The exemption is aimed at circumstances in which knowledge of otherwise unknown or obscure investigative or prosecutorial techniques or guidelines can be reasonably expected to facilitate violations of the law or evasion of the consequences of such violations.[3]

Here, even if ICE had established that the database information sought by plaintiffs would reveal something about the investigative or prosecutorial techniques or guidelines ICE uses in immigration law enforcement proceedings (which, as explained above, it has not), the "circumvention of the law" that it claims is likely is not attributable to any disclosure of such techniques or guidelines, as the statute

[3] *See*, *e.g.*, *Ferri v. Bell*, 645 F.2d 1213, 1224 (3d Cir. 1981); *Blanton v. U.S. Dept. of Justice*, 63 F. Supp. 2d 35, 49–50 (D.D.C. 1999); *Albuquerque Pub. Co. v. U.S. Dept. of Justice*, 726 F. Supp. 851, 857–58 (D.D.C. 1989).

requires. ICE claims, instead, that disclosure of the *structure of its databases* could be useful to persons who might wish to engage in unlawful cyberattacks targeting the databases. The structure of a database that contains information about pending matters, however, is not itself an investigative or prosecutorial technique.

Thus, there is a fundamental disconnect between the harm required by Exemption 7(E)—a risk of circumvention of the law *attributable to disclosure of enforcement or prosecutorial methods*—and that claimed by ICE in this case—a risk to data security supposedly threatened by disclosure of the design of a database. Exemption 7(E) reflects Congress's deliberate choice to provide an exemption applicable only where the former risk is shown. *See Milner*, 131 S. Ct. at 1267–68. Almost any information could conceivably be of use to a potential criminal, but Congress has not seen fit to create a broad exemption for all such risks, only for the special circumstances when evasion of the law could result from disclosure of methods and criteria the government uses to investigate and prosecute cases. That is not the risk the government asserts here, so Exemption 7(E) is inapplicable.

C. The government has not shown a genuine risk of harm.

Even if the possibility of cyber-attacks that the government posits were the type of risk at which Exemption 7(E) is directed (circumvention of law attributable to disclosure of investigative or prosecutorial techniques or guidelines), the government has failed to carry the burden of demonstrating that the harms it fears "could reasonably be expected" to result from disclosures about the structure of its

databases. 5 U.S.C. § 552(b)(7)(E). Disclosure of the structure of the databases makes such attacks no more likely to occur or succeed than nondisclosure.

As demonstrated by the declaration of Dr. Paul Clark, the type of attack the government fears could occur only if there were a means of external access to the databases—that is, an accessible web interface—which does not exist. And even if such an interface existed, the widely accepted best practices for prevention of an attack would include such measures as firewalls, password protections, and protocols designed to ensure that unauthorized commands will not be executed. By contrast, seeking to prevent attacks by maintaining secrecy about the contents or structure of databases—"security through obscurity"—is not an accepted means of protecting information. *See* Clark Dec. ¶¶ 12–17 (Doc. 18-3).

The government admits its databases are not accessible to an external attacker or to anyone outside the Department of Homeland Security. Defendants' Response to Plaintiff's Statement of Material Facts, ¶¶ 21–22 (Doc. 25-6). The government's response to the point that an attack cannot occur without a means of access to the databases is that data breaches can occur in the absence of a publicly accessible web interface. The sole support the government offers for this assertion is that the Home Depot data theft did not make use of a web connection to a database. Wilson Supp. Dec. ¶ 9 (Doc. 25-1). ICE is correct that that data breach involved the theft of data using another means of access—point-of-sale credit card readers. Obviously, however, the information in the ICE and CBP databases cannot be accessed using such means, and the government does not suggest that they can. The government's exclusive

reliance on such an obviously inapt example underscores that a cyber-criminal has no comparable way to obtain the access to its databases that would be necessary for the type of attack the government claims to fear. *See* Second Clark Dec. ¶¶ 3–4 (filed herewith). The government has failed even to suggest how such access could occur, let alone demonstrate that it would be reasonably likely to occur.

The rest of the material provided by the government with its latest round of briefing confirms Dr. Clark's point that ICE and CBP employ robust protections for data, including firewalls, passwords, and other means of ensuring that unauthorized access is not permitted and unauthorized commands are not executed. *See id*. at ¶¶ 5–7. On top of those measures—which the government does not contend would be compromised by the information requested—maintaining secrecy as to the names and contents of database tables and fields would add nothing to the security of the databases. Such information would not assist a cyber-criminal in obtaining a connection to the databases or bypassing firewalls and security measures. *Id*. at ¶¶ 7–9. Moreover, an attacker who managed to obtain access to the databases, penetrated the firewalls, cracked password protection, and bypassed measures to prevent unauthorized commands would obtain access to the database schema and code tables that identify fields within the database. *Id*. at ¶ 9. The insertion of malicious software does not require *advance* knowledge of the contents of a database. *Id*. Thus, the disclosures sought in this case could not reasonably be expected to increase whatever risk of cyber-attack may exist in light of the strong protections of this data. *Id*.

That the disclosure of information about the structure of the database cannot reasonably be expected to risk cyber-attacks is strongly reinforced by the government's routine disclosure of similar information in a variety of settings. ICE itself has repeatedly disclosed names of tables and fields in the EID database, even while maintaining in this case that such disclosure poses a risk of harm. Second Long Dec. ¶¶ 4, 6–8 (filed herewith). Mr. Wilson's assertion that *he* is unaware of or did not authorize those releases, Wilson Supp. Dec. ¶ 7, does not alter the fact that the agency determined that the material was releasable, in one instance as part of the resolution of litigation. Second Long Dec. ¶ 3. Likewise, the Department of Justice routinely releases information about its case management databases (which similarly contain information about pending investigations and prosecutions), including the names of tables and fields within those tables (not to mention the data itself). Second Long Dec. ¶¶ 9–10; Second Hasan Dec. ¶¶ 9–10 (filed herewith). If ICE's arguments in this case were correct, all that information would fall within Exemption 7(E) and would pose a threat to the security of the Justice Department's data. The Justice Department evidently sees no such threat.

The government's arguments, if accepted, would result in the effective denial of access to electronically stored data concerning any government enforcement proceedings. Making sense of the information stored in a relational database necessarily requires understanding the identity of the tables and fields into which that data is organized, and how they relate to one another. Absent that information,

the data itself, although non-exempt under FOIA, would become unusable and meaningless, rendering FOIA requests for the data futile. Second Long Dec. ¶ 10.

II. The new Exemption 7(A) claim lacks merit.

For the first time, ICE has asserted that withholding information concerning the structure of its databases is authorized by Exemption 7(A), which applies to law enforcement records whose production "could reasonably be expected to interfere with law enforcement proceedings." ICE's new claim lacks legal and factual merit.

ICE's argument rests on the fact that its databases contain "information pertaining to cooperating witnesses, seizure identifiers, fugitive status, and alerts," Pineiro Supp. Dec. ¶ 16, and the assertion that disclosure of such information could interfere with pending investigations. ICE, however, is objecting not to the disclosure of the information itself (which could be redacted if ICE were actually to produce the database snapshots sought by plaintiffs). It objects instead to disclosure of the database schema and other information about the structure of the database. ICE does not contend that that information, which it describes as "metadata," contains names of witnesses, fugitives, or other information about any particular pending investigation. Rather, relying on the same arguments it makes about Exemption 7(E), ICE contends that disclosure of the database schema could assist someone who managed to obtain access to its database and bypass its security measures in finding such information in the database, compromising some investigation.

In other words, the "production of [the] records" requested could not "reasonably be expected to interfere with enforcement proceedings," as Exemption

7(A) requires, but only the government's hypothetical failure to secure its databases against intrusion. The exemption thus does not apply. As the D.C. Circuit has long recognized, Exemption 7(A) requires the government to "show something *more* than a direct relationship between agency records and a pending investigation"; it must demonstrate "how the *particular kinds of investigatory records requested* would interfere with a pending enforcement proceeding." *Campbell v. Dept. of Health & Human Servs.*, 682 F.2d 256, 261, 259 (D.C. Cir. 1982) (emphasis added); *see also CREW*, 746 F.3d at 1098–99. The government's showing must "focus upon categories of records encompassed by [plaintiff's] request" and "must demonstrate specifically how each document or category of documents, if disclosed, would interfere with the investigation, for example, how revelation of any particular record or record category identified as responsive to [plaintiff's] request would reveal to particular targets, actual or potential, the scope, direction, or focus of the [agency's] inquiry." *Campbell*, 682 F.2d at 265. Here, the government has not even met the threshold requirement of showing a *direct* relationship between disclosing information about the structure of its database and interference with specific pending enforcement proceedings, let alone shown how the *particular information requested*—that is, information about the structure of its database—would itself interfere with any proceedings. The government does not even contend that the particular records requested would themselves reveal anything that would interfere with a pending investigation.

On the government's expansive theory, it could withhold information about the location of its file repositories under Exemption 7(A)—even though that

information in itself would reveal nothing that could interfere with any pending proceeding—on the supposition that a burglar who broke into a government building might use it to find information in the files that revealed the name of a witness in a pending proceeding. The government cites no decision that gives Exemption 7(A) such expansive scope. Moreover, the government's position is contrary to the routine practice of other government agencies, including the Department of Justice itself, which has disclosed the structure of its case management databases in response to FOIA even though those databases similarly contain information that, if disclosed, might affect ongoing proceedings. *See* Second Long Dec. ¶¶ 9–10; Second Hasan Dec. ¶¶ 9–10. Unlike ICE here, DOJ has properly relied on withholding or redaction of specific entries in its databases to protect such information, not concealment of the structure of the databases themselves.

ICE's argument fails not only legally, but also factually. The claim is based on the farfetched supposition that a target of some ICE investigation, armed with the database schema and other information disclosed in response to the FOIA requests at issue, would hack into ICE's system and discover the names of potential witnesses, information about a fugitive alert, or some other information that would compromise the investigation. Like ICE's Exemption 7(E) claims, that supposition founders on ICE's failure to demonstrate that, in light of the lack of an interface that would allow external access to its databases and the other security measures it employs, concealing the structure of its databases would add appreciably to the security of the underlying data. *See* Second Clark Dec. ¶¶ 3–9.

III. ICE's invocation of Exemption 3 is meritless.

In opposing plaintiffs' summary judgment motion, ICE for the first time contends that information about its databases falls within FOIA's Exemption 3, covering records "specifically exempted from disclosure by statute." 5 U.S.C. § 552(b)(3). Exemption 3 applies only if a statute "requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue" or "establishes particular criteria for withholding or refers to particular types of matters to be withheld." *Id*. A statute "enacted after the date of enactment of the OPEN FOIA Act of 2009"—October 28, 2009—is an Exemption 3 statute only if it "specifically cites to" 5 U.S.C. § 552(b)(3). *Id*.

ICE's Exemption 3 claim fails because the statute it invokes was repealed in 2014 and replaced by another statute that does not specifically cite § 552(b)(3). The purported Exemption 3 withholding statute is the Federal Information Security Management Act (FISMA), which was enacted as Title II of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, and was codified at 44 U.S.C. §§ 3541–3549. On December 18, 2014, those provisions were repealed in their entirety by the Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073, and replaced by a new set of information security provisions codified at 44 U.S.C. §§ 3551–3558. The current statute postdates the enactment of the OPEN FOIA Act of 2009, and nowhere contains a specific citation to 5 U.S.C. § 552(b)(3). It therefore is not an Exemption 3 statute.

Even leaving aside the absence of a specific citation to § 552(b)(3), the statutory provisions concerning federal information security could not exempt any records from disclosure under FOIA because *they expressly state that they do not affect disclosure under FOIA*. Specifically, 44 U.S.C. § 3558, entitled "Effect on existing law," provides that "[n]othing in this subchapter … may be construed as affecting the authority of … the head of any agency, with respect to the authorized use or disclosure of information, including with regard to … the disclosure of information under section 552 of title 5." The law is thus an *anti-Exemption 3* statute: It explicitly does *not* exempt records from disclosure under FOIA. A law that expressly says it does not affect disclosure under FOIA cannot give rise to a statutory exemption claim under FOIA. *Cf. Public Citizen, Inc. v. Rubber Mfrs. Assn.*, 533 F.3d 810, 814–15 (D.C. Cir. 2008) (holding that a statute prohibiting only disclosures in *addition* to those required under FOIA was not an Exemption 3 statute). Notably, the repealed statute ICE invokes contained exactly the same disclaimer of any limit on agency authority to disclose information under FOIA. *See* former 44 U.S.C. § 3549 (2014).

Even if the statute currently in force did not fail the threshold test of referencing Exemption 3, and even if it (like its predecessor) did not specifically disclaim any effect on authorized disclosures under FOIA, ICE points to no specific authorization in the statute for the withholdings at issue. Instead, ICE points to the former statute's general statement of its purposes and its broad definitions of certain terms (which roughly correspond to current 44 U.S.C. §§ 3551 & 3552), none of which require, or set forth specific criteria for, withholding records. ICE also cites

former § 3543, which conferred certain responsibilities on the Director of the Office of Management and Budget. The current statute replaces that section with § 3553, which delegates authority to the Director of OMB and the Secretary of the Department of Homeland Security. But ICE does not identify any directive or other action taken by the Director or the Secretary pursuant to § 3553 (or, for that matter, its now repealed predecessor) that requires withholding of these records. Finally, ICE refers to former § 3544, which generally made agency heads responsible for information security. That section has been replaced by § 3554, which states broadly that agency heads are responsible for "providing information security commensurate with the risk and magnitude of the harm resulting from *unauthorized* access, use, disclosure, disruption, modification, or destruction" of information or information systems (emphasis added). That generally worded responsibility to prevent *unauthorized* access provides no authority to restrict disclosure of records under FOIA—it does not meet the "threshold requirement" that it "specifically exempt" records from disclosure authorized by FOIA. *Public Citizen*, 533 F.3d at 815; s*ee CNA v. Donovan Fin. Corp.*, 830 F.2d. 1132 (D.C. Cir. 1987) (18 U.S.C. § 1095's prohibition of unauthorized disclosure of trade secrets is not an Exemption 3 statute).

IV. ICE's contention that the request for database snapshots falls outside FOIA because it would require creation of a new record is meritless.

A. Providing copies of the snapshots would not involve creation of new records.

With respect to plaintiffs' request for copies of the snapshots of parts of the EID database that ICE creates on a regular basis, ICE does not claim that the

snapshots fall within any FOIA exemption, but argues that the requests for snapshots fall outside FOIA altogether because they ask ICE to create new records, which FOIA does not require it to do. ICE's argument is meritless: The requests seek exact copies, in an electronic format, of the EID snapshots that make up the IIDS database and other agency "datamarts." The IIDS database and other datamarts are agency records within the meaning of FOIA and are in turn exact copies of portions of the EID database, also an agency record. *See* 5 U.S.C. § 552(f)(2)(A) (defining a record as "any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format"). The Electronic Freedom of Information Act Amendments of 1996 provide specifically that an agency shall provide requested records "in any form or format requested by the person if the record is readily reproducible by the agency in that form or format." *Id*. § 552(a)(3)(B). That mandate forecloses ICE's argument by making clear that copying database tables and providing them in an electronic format specified by a requester is a way of making *existing* agency records available as required by FOIA, not creation of new records.

ICE argues that when it extracts portions of the EID database and transmits them as snapshots to the IIDS database (and others), it does not retain "specific extract files or intermediate entities," Wilson Dec. 8 (Doc. 17-6), and, therefore, providing a copy of the EID tables in the snapshots would create a new record that does not otherwise exist. But ICE does not dispute that the snapshots have a separate existence in the IIDS database and the other datamarts until they are replaced by

more current snapshots. ICE does not contend that making copies of those databases would be impossible. Such copies would satisfy the requests for current snapshots,[4] and would replicate existing records: the IIDS database and other datamarts, as well as the corresponding EID tables. *See* Second Hasan. Dec. ¶ 3.

Courts have consistently held that making exact copies of existing electronic records is not creation of a new record, even if it involves using computer programs to select the data elements to be included and modifying the records' format. Where an agency "possesses in its databases the discrete pieces of information which [the requester] seeks, extracting and compiling that data does not amount to the creation of a new record." *Schladetsch v. U.S. Dept of Housing & Urban Dev.*, 2000 WL 33372125, at *3 (D.D.C. April 4, 2000). "[S]orting a pre-existing database of information to make information intelligible does not involve the creation of a new record because, as Congress noted in the legislative history to the E-FOIA Amendments, '[c]omputer records found in a database rather than a file cabinet may require the application of codes or some form of programming to retrieve the information.'" *Nat'l Sec. Counselors v. CIA*, 898 F. Supp. 2d 233, 270 (D.D.C. 2012) (quoting H.R. Rep. 104-795, at 22 (1996)). Thus, a request that seeks "entire fields of data from particular electronic databases" is proper under FOIA, and as long as the

[4] The government briefly repeats its claim that it cannot provide the requested snapshots because the ones that were current when the requests were made no longer exist. Opp.-Reply 1. As plaintiffs' opening memorandum explained (at 27), the requests are not limited to information existing on the date of the requests, but seek the most recent snapshot as of the time the government complies. The government does not respond to the arguments and authorities cited by plaintiffs on this point.

requester seeks "the contents of the database"—as opposed to an analysis of the data, or other information that does not otherwise exist—FOIA requires production. *Id*. at 271. Indeed, production is required even though it might be more burdensome than creating a record, which FOIA does not require. *See id*. at 272. In short, compliance with plaintiffs' requests for copies of snapshots would not create a "new database," but only a new *copy* of an existing database.

B. The government has not shown that it would not be feasible to produce the records requested.

Under FOIA, an agency is required to provide records in electronic form if they are "readily reproducible by the agency in that form.""5 U.S.C. § 552(a)(3)(B). The ease of reproducing electronic records has led this Court to conclude that records maintained electronically are readily reproducible in that form except in "highly unusual" cases. *Scudder v. CIA*, 25 F. Supp. 3d 19, 38 (D.D.C. 2014). Here, ICE's argument that the EID tables the snapshots comprise are not readily reproducible is unfounded. The functionality for extracting and copying database tables is built into database management software, Hasan Dec. ¶ 10 (Doc. 18-4), and ICE does not deny that it uses such software—as is evident from the fact that it regularly extracts tables from the EID database and provides them to various governmental users.

Moreover, the government has provided copies of EID and IIDS tables to the plaintiffs on many occasions, including at least one exact copy of an EID table including the table's name and that of each field of information within it. Second Long Dec. ¶¶ 3–4; Long Dec. ¶ 16 (Doc. 18-2). ICE's declarant professes not to know the circumstances in which ICE provided that table, Wilson Supp. Dec. ¶ 7, but his

lack of knowledge does not alter the fact that the production of the table evidences ICE's ability to provide copies of tables. In addition, ICE has produced millions of data records from EID tables over the past five years. Second Long Dec. ¶ 5. In many instances those productions were in spreadsheet format, *see id.*, but contrary to the government's argument, reproducing data extracted from a database is production of a *copy* within the meaning of FOIA, not creation of a new record, regardless of the particular format in which it is produced. *Nat'l Sec. Counselors*, 898 F. Supp. at 270–72. The spreadsheets were copies under FOIA because they reproduced the exact data entries in the original EID tables. Second Long Dec. ¶ 5.[5]

That ICE has produced copies of database tables in the past establishes that they are readily reproducible in electronic form. ICE contends that the greater volume of the records requested here somehow makes reproducing them in their entirety infeasible. As plaintiffs' declarant Michael Hasan explains, the task of reproducing large numbers of tables is no more technically difficult than reproducing one. Put another way, if one table can be copied, so can 1,000; it is merely a matter of identifying the tables to be included and copying the data. That the *volume* of data may be large, even measurable in terabytes, does not mean that copying—an

[5] The altered descriptions of fields that ICE inserted into those spreadsheets in place of the original field names were not themselves agency records whose production could be compelled under FOIA, but that is irrelevant here, because plaintiffs do not ask ICE to create altered records, only to provide the real field names in conjunction with copies of the data.

automated process once the relevant tables are identified—is burdensome. *See* Second Hasan Dec. ¶ 2; Hasan Dec. ¶¶ 11; *see also* Second Long Dec. ¶ 11.

ICE asserts that Mr. Hasan has never worked for the government, but that is beside the point in a number of respects. First, the technical process of copying a table in an Oracle database does not depend on whether the database is owned by the government or by a private entity. Second Hasan Dec. ¶ 9; Hasan Dec. ¶ 10.[6] Second, although Mr. Hasan has not worked for the government, he has worked extensively with the government on the details of production of similar databases from other agencies, including the Department of Justice. Based on that experience, he has personal knowledge that it is indeed possible for the government to provide copies of large numbers of tables from massive databases—indeed, essentially entire databases other than specific exempt material they contain—to private requesters. Second Hasan Dec. ¶¶ 5–9. *Cf.*, *e.g.*, *TPS, Inc. v. Dept. of Def.*, 330 F.3d 1191, 1196 (9th Cir. 2003) (holding that a declaration that a private entity received information in a particular electronic form from the government was evidence of the government's ability to provide it in that form); *Scudder*, 25 F. Supp. 3d at 40 (same). Third, to the extent the obstacles to production the government identifies are the result of its own bureaucratic oversight requirements rather than actual limits of technology, its self-imposed need to comply with protocols in the production of information does not

[6] The government, without denying that the databases are Oracle databases, says that Mr. Hasan merely "presumes" that is the case. Opp.-Reply 15. Information previously produced to plaintiffs, however, confirms that the databases are Oracle databases. Long Dec., Exh. I.

constitute a burden excusing it from its FOIA obligations. *See Public.Resource.org v. IRS*, 2015 WL 393736, at *4 (N.D. Cal. Jan. 29, 2015).

Beyond its claim that copying the data is infeasible, ICE contends that it lacks a means to redact exempt information from the database. ICE has not identified specific exemptions to which it believes the data itself is subject (in contrast to its claims of specific exemption for information about the structure of the databases, addressed above). In any event, the contention that large databases cannot feasibly be redacted is not credible. As Mr. Hasan has explained, redaction involves identifying fields in which information is exempt and executing programs to redact those fields. Second Hasan Dec. ¶ 4; Hasan Dec. ¶ 13–14. That the quantity of data may be large—whether 6.7 billion lines or comparable to 1.8 million songs on an iPod—is no obstacle to the performance of that function. *Id*. ICE itself has redacted data from its previous voluminous releases of data from the EID by replacing entries in some columns with redaction symbols, even when the tables included a million rows of data. Second Long Dec. ¶ 5. The experience of other agencies is likewise instructive: As Mr. Hasan and Ms. Long explain, TRAC regularly receives massive databases from government agencies, including DOJ's civil and criminal case management databases, in which such processes are routinely used to redact fields containing assertedly exempt information. Second Hasan Dec. ¶¶ 7–8.

ICE argues, however, that it currently lacks the software used by other agencies to perform such redaction. ICE's assertion is not credible both because it has redacted information from the data it has produced to plaintiffs in the past and

because redaction is a built-in function of standard database management software. Second Hasan Dec. ¶ 4; Hasan Dec. ¶ 13. In any event, ICE cites no authority supporting the proposition that its lack of redaction software excuses it from its obligation to produce segregable, non-exempt information that it maintains in electronic form. An agency cannot exempt itself from FOIA's requirements that it make its electronic records available upon request by denying itself the means to separate exempt and non-exempt records. *See Public.Resource.org*, 2015 WL 393736, at *2–*4.

Finally, the government has made no similar claims that CBP lacks the ability to produce and redact copies of the databases under its control, including EID extracts provided for the CBP data warehouse. The government has provided no claims of either feasibility or exemption supporting the withholding of that data.

C. The government cannot evade FOIA by maintaining records electronically.

Ultimately, the government's contention here is not just that it is not feasible to provide the records requested in the form sought by plaintiffs, but that it need not provide them in *any* form. That position is not supported by any provision of FOIA and would have extremely troubling implications. In effect, accepting the government's positions would mean that by maintaining the official records of its actions in the form of an electronic database, the agency has put them outside the scope of FOIA. That consequence would turn FOIA, especially as modified by the E-FOIA Amendments, on its head.

V. The government's search was not adequate.

As explained in plaintiffs' opening memorandum (at 31), the government has provided no explanation of the nature of any search conducted for requested records concerning the preparation of extracts of EID data. The government's Opposition-Reply does not address this point at all: It says nothing about the search for these records. Nor does its assertion that it was excused from searching because all requested records would be subject to Exemption 7(E) apply to this category of records. Even if the government were correct that records concerning the structure of its databases posed some security risk that fell within the scope of that exemption, it has offered no argument concerning how records saying when it prepared extracts of the EID data and what agency components prepared and received them would present any similar risk. The agency's failure to explain what search it conducted for these records—even when its FOIA office had remanded for a further search, *see* Long Dec. ¶ 6—requires a finding that its search was inadequate in this respect.

The government also concedes that ICE did not search the EID database (or the other databases that contain snapshots of EID data) for records responsive to requests for the database schema and code tables. It argues that such a search was unnecessary because it searched other locations, and searching a database itself for records setting forth its structure would be like searching a building in order to reconstruct its blueprints. Wilson Supp. Dec. ¶ 17. The government's analogy is flawed, however, because a relational database necessarily contains records providing the database schema and code tables. Second Hasan Dec. ¶ 10. Indeed, the

government's declarant Karolyn Miller acknowledged this point in her October 8, 2014 declaration, at ¶ 10 (Doc. 17-1). Locating and copying the responsive information from the databases would require only the execution of simple commands, and would provide the most accurate and current records responsive to the requests for database schema and code tables. Second Hasasn Dec. ¶¶ 9–10. The government's failure to search the databases renders its search inadequate.

The government likewise concedes that CPB conducted no search for responsive records, even though CBP uses the databases in question and maintains its own data warehouse that receives snapshots of EID tables. The government does not argue that CPB would possess no responsive records, but relies on its assertions that ICE "owns" the EID database, Wilson Dec. 3, and that its system lifecycle management (SLM) repository is the "official place" for records requested by plaintiffs. Wilson Supp. Dec. ¶ 17. The responsibility to search for records that are responsive to a FOIA request is not determined by such formal categories as "ownership" or "official" repositories, but by whether a search of a location would be "reasonably calculated to discover the requested documents." *SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197, 1201 (D.C. Cir. 1991); *see also Public Citizen, Inc. v. Dept. of Educ.*, 292 F. Supp. 2d 1, 8 (D.D.C. 2003); *Judicial Watch, Inc. v. U.S. Secret Serv.*, 579 F. Supp. 2d 143, 150 (D.D.C. 2008).[7] In light of CBP's use of the databases in

[7] Even if "ownership" were relevant, both ICE and CBP have acknowledged that CBP "owns" and controls some parts of the EID, Second Long Dec. ¶¶ 12–14, and, in any event, CBP has a data warehouse with EID extracts related to certain arrests and prosecutions. Long Dec., Exh. F, at 2.

question, and its regular receipt of EID extracts for its data warehouse, it would be implausible to suggest that CBP possesses no potentially responsive documents, and the government does not in fact assert that it does not. The government has thus failed to justify CBP's failure to search for records.

Finally, the government contends that the scope of its search does not matter because all records within the scope of plaintiffs' request are categorically exempt under Exemption 7(E). As explained above, however, the government's Exemption 7(E) theory is meritless. Moreover, even if *some* of the requested records did fall within Exemption 7(E), the government's contention that *all* records related to its databases are categorically exempt under Exemption 7(E) is patently overbroad.

CONCLUSION

For the foregoing reasons, the Court should grant plaintiffs' motion for summary judgment.

/s/ Scott L. Nelson
Scott L. Nelson
DC Bar No. 413548
PUBLIC CITIZEN LITIGATION GROUP
1600 20th Street NW
Washington, DC 20009
(202) 588-1000

March 30, 2015 *Counsel for Plaintiffs*

CERTIFICATE OF SERVICE

I hereby certify that the foregoing Reply Memorandum in Support of Plaintiffs' Motion for Summary Judgment and accompanying materials were served on counsel for the defendants via the court's electronic filing system on March 30, 2015.

/s/ Scott L. Nelson
Scott L. Nelson